DIGITAL IDENTITY

Ben Livshits, Microsoft Research

Overview of Today's Lecture

- Brief history of user identities
- Single sign-on
- Federated identity model
- Popular identity protocols
  - SAML
  - OpenID
  - InfoCard and CardSpace

A Brief History of Identities

▸Learn the discipline, pursue the art, and contribute ideas at www.ArchitectureJournal.net

Resources you can build on.

THE ARCHITECTURE JOURNAL

Input for Better Outcomes

Journal 16

Identity and Access

The Evolving Role of the Identity

Federated Identity Patterns in a Service-Oriented World

Managing Identity Trust for Access Control

Architecture Journal Profile: Kim Cameron

Federated Identity and Healthcare

Claims and Identity: On-Premise and Cloud Solutions

Enterprise Identity Synchronization Architecture

Microsoft

- □ In the beginning...
- □ … there was almost no interest in creating and managing identities and their security contexts. Why? We lived in a world of mainframes and mini-computers, submitting huge computational jobs through punched cards and printing stacks and stacks of paper on mechanical printers (but only if we were IT professionals or attending University classes at that time). Our identity was nothing more than an **identifier**, determining who **submitted the job** and who owned that big amount of paper (usually, printed on the first page of the paper stack).
- □ There was no **security context** at all in our identities. The user name/password pair was even printed in the punched card set, so that there was absolutely no secrecy involved. However, there was no need for it, especially in the commercial/academic world; except for a few individuals, there was no interest in stealing other people's jobs (JCL jobs, that is). The only necessary **secrets** were in the realm of military installations. Identities were used only in the context of a single machine. If you wanted to use another computer, another user name/password pair had to be created, and there was no connection among the identities in the machines that you were allowed to use.
- □ Basically, identities were not used to really **identify** you. Their only purpose was to generate an identity under which a process was run and the results could be **sent** to you. There was a very weak connection between you and your **digital identity**.

A Brief History of Identities

□ With the advent of distributed computing, network **logon** became a necessity, and technologies and protocols were specially created to handle
those needs. But
computers to the
were really a set
presenting the in
only a view of the
resources but, wh
the local identity
workgroup memb
were correct.

□ The workgroup c
servers became p
identity database
credentials' valid
quickly as we cou
up in our lives. Th
unique entity am
a printer, no mat
myself using my s
first years of the
artifact was used
a known and trus
implementing the
Obviously, this m
number of server
commonplace.

□ This may have be
relationship betw
the same set of credentials (user name/password) were used to access a set of network resources.

□ Then came the concept of the network domain. In it, a set of workstations and servers are managed under a central credential
a common security context
cesses. In the **network**
orkstations, and services
execution of processes
edentials will validate only
ain.

elationships between
trolled by domain A can
domain B is set to trust the
ore flexible identity
eplicate or clone identities
nship has been previously

nains that are part of the
gies, making it very difficult
ectories or directories from

andardized to handle the
coupled network domains.
n systems: A predefined,
designed exclusively to
etwork domain to share
e sets of standards-based
cture, allowing the sharing
network links.

phs, digital identities had to evolve from a single pair of user name/password to a very **complex set** of **protocols** that transport lots of user-related **claims** and **attributes**.

□

New sets of technologies were created and standardized to handle the transmission of user identities among **loosely coupled network domains**. They are collectively called **identity-federation systems**: A predefined, cross-platform, standardized set of protocols designed exclusively to transmit user security contexts to allow one network domain to share resources with another network domain. These sets of standards-based protocols are friendly to the **Internet infrastructure**, allowing the sharing of resources even in the absence of dedicated network links.

As can be inferred from the preceding paragraphs, digital identities had to evolve from a single pair of user name/password to a very **complex set** of **protocols** that transport lots of user-related **claims** and **attributes**.

Basic Motivating Scenario

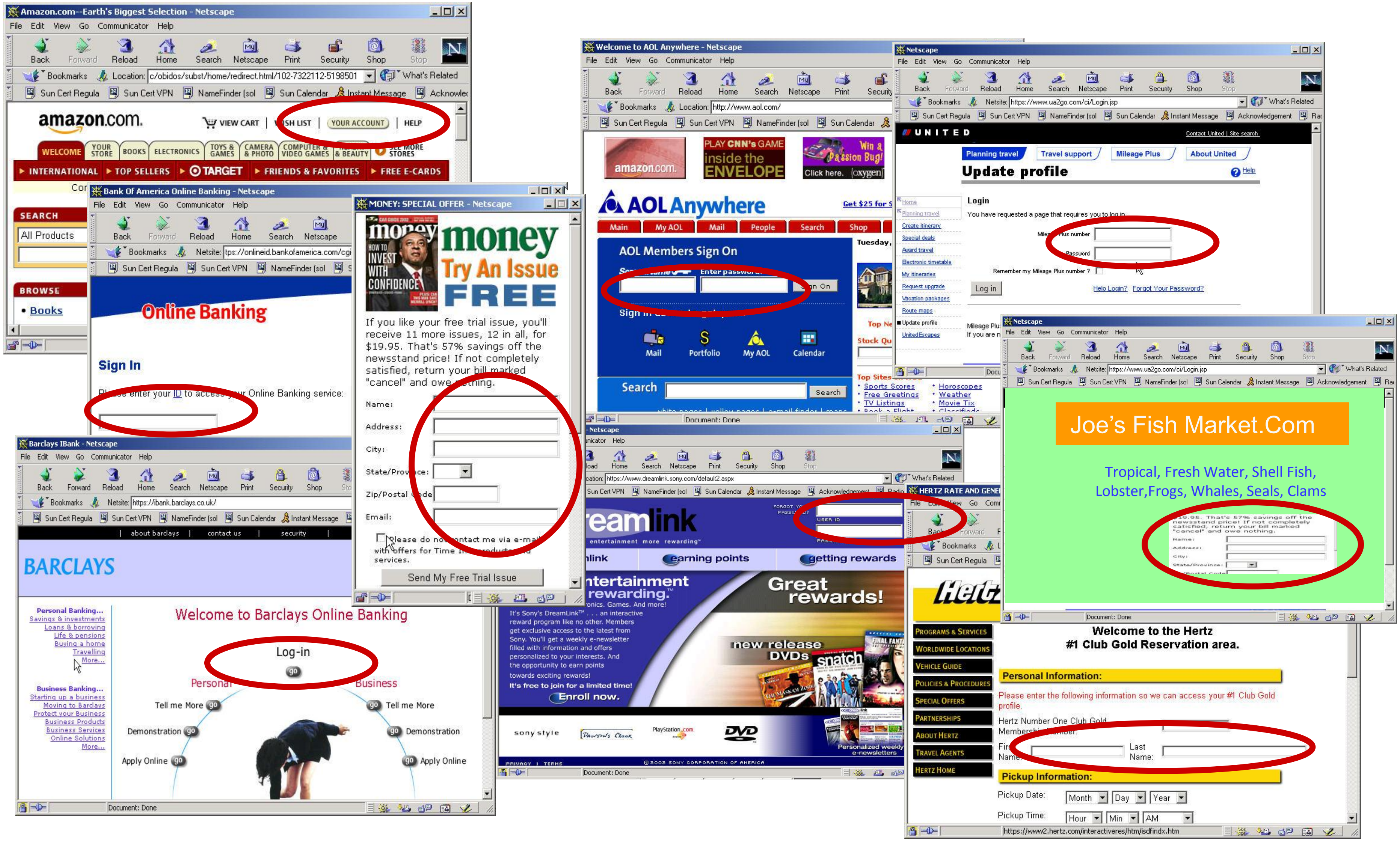
- The user is going to travel
- …or shop
- …or blog

- Tasks
  - Sign in for booking flight ticket
  - Sign in for booking hotel room
  - Sign in for renting a car

Single Sign-On (SSO)

in a **client/server** relationship, single sign-on is a session/user **authentication** process that permits a user to enter one name and password in order to access multiple applications

Ongoing Identity Crisis



Amazon.com--Earth's Biggest Selection - Netscape

Location: c/obidos/subst/home/redirect.html/102-7322112-5198501

Bank Of America Online Banking - Netscape

Netsite: tps://onlineid.bankofamerica.com/cgi

Online Banking

Sign In

Pl... se enter your ID to access ...ur Online Banking service:

MONEY: SPECIAL OFFER - Netscape

money Try An Issue FREE

If you like your free trial issue, you'll receive 11 more issues, 12 in all, for $19.95. That's 57% savings off the newsstand price! If not completely satisfied, return your bill marked "cancel" and owe nothing.

Name:

Address:

City:

State/Province:

Zip/Postal Code:

Email:

□ Please do not contact me via e-mail with offers for Time Inc. products and services.

Send My Free Trial Issue

Barclays IBank - Netscape

Netsite: https://ibank.barclays.co.uk/

BARCLAYS

Welcome to Barclays Online Banking

Log-in

Welcome to AOL Anywhere - Netscape

Location: http://www.aol.com/

AOL Members Sign On

Enter password

Netscape

Netsite: https://www.ua2go.com/ci/Login.jsp

UNITED

Update profile

Login

You have requested a page that requires you to log in.

Mileage Plus number

Password

Remember my Mileage Plus number ?

Log in

Help Login? Forgot Your Password?

Netsite: https://www.ua2go.com/ci/Login.jsp

Joe's Fish Market.Com

Tropical, Fresh Water, Shell Fish, Lobster,Frogs, Whales, Seals, Clams

https://www.dreamlink.sony.com/default2.aspx

dreamlink

It's Sony's DreamLink™ . . . an interactive reward program like no other. Members get exclusive access to the latest from Sony. You'll get a weekly e-newsletter filled with information and offers personalized to your interests. And the opportunity to earn points towards exciting rewards!

It's free to join for a limited time!

Enroll now.

HERTZ RATE AND GENERAL

Welcome to the Hertz #1 Club Gold Reservation area.

Personal Information:

Please enter the following information so we can access your #1 Club Gold profile.

Hertz Number One Club Gold Membership Number:

First Name:

Last Name:

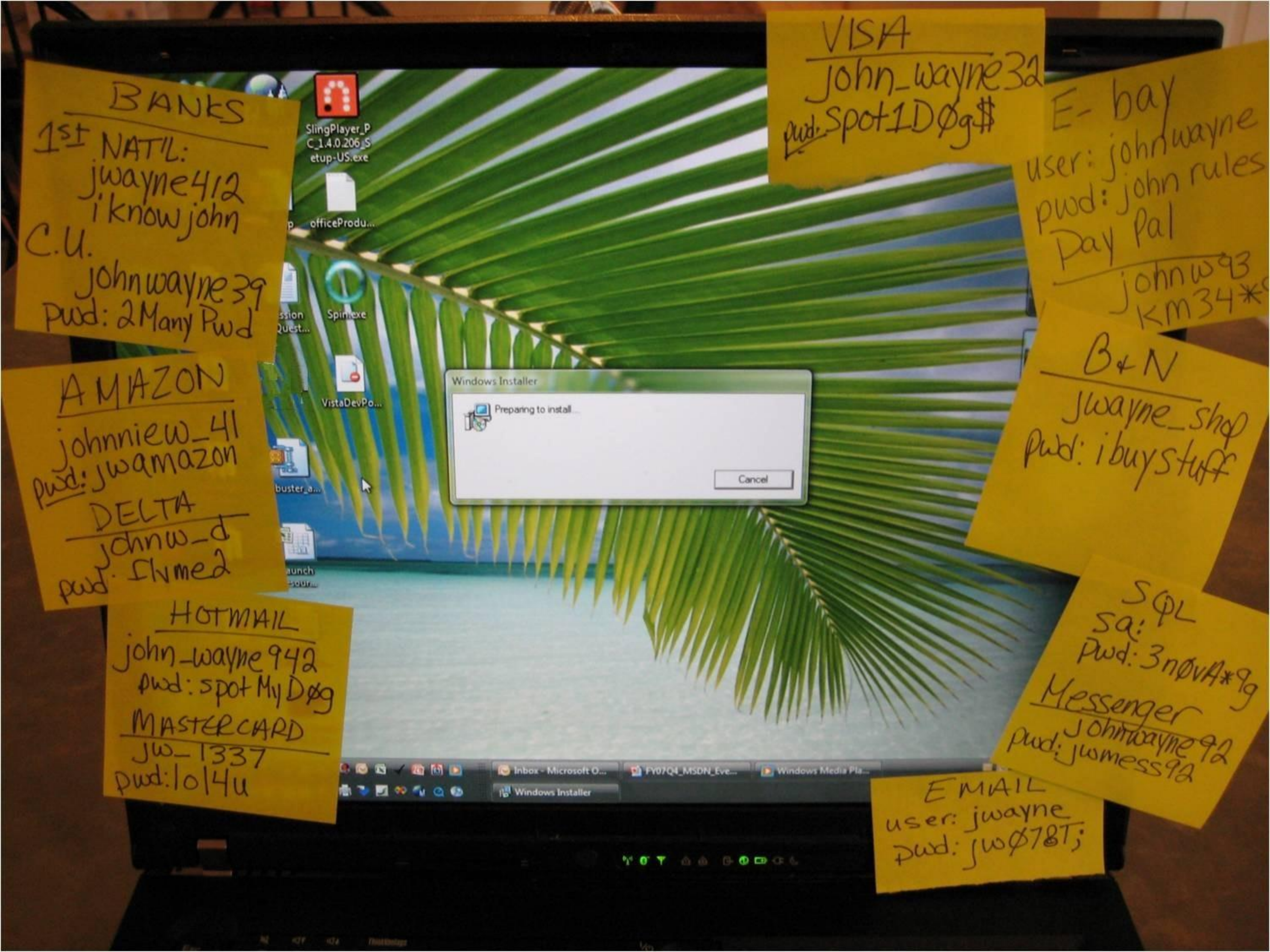
Pickup Information:

Pickup Date: Month Day Year

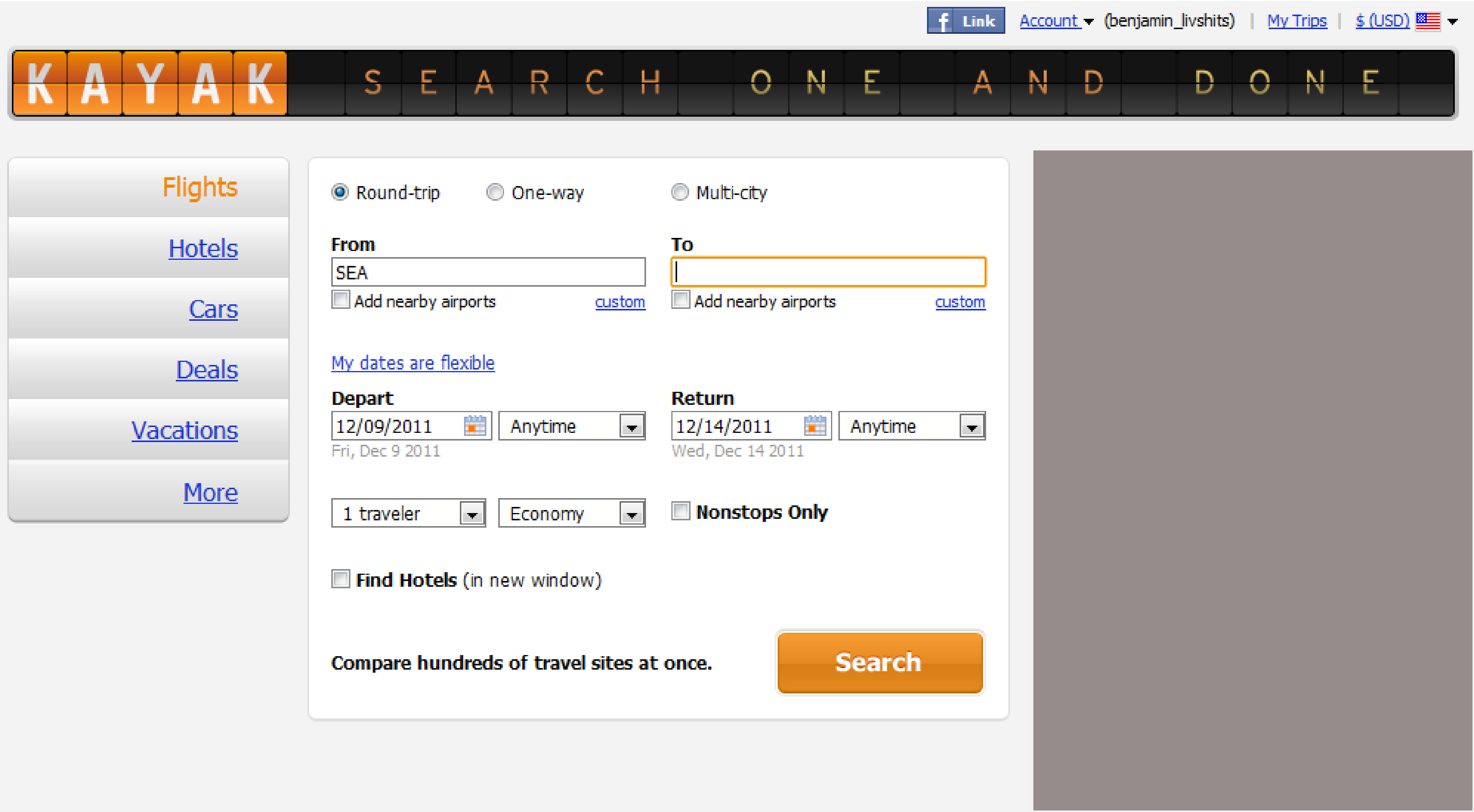
Pickup Time: Hour Min AM

https://www2.hertz.com/interactiveres/html/isdfindx.htm

File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks
What's Related
Sun Cert Regula Sun Cert VPN NameFinder (sol Sun Calendar Instant Message Acknowledgement
VIEW CART | WISH LIST | YOUR ACCOUNT | HELP
WELCOME YOUR STORE BOOKS ELECTRONICS TOYS & GAMES CAMERA & PHOTO COMPUTER & VIDEO GAMES SEE MORE STORES
INTERNATIONAL TOP SELLERS TARGET FRIENDS & FAVORITES FREE E-CARDS
SEARCH
All Products
BROWSE
Books
Personal Business
Tell me More
Demonstration
Apply Online
about barclays contact us security
Main My AOL Mail People Search Shop
Mail Portfolio My AOL Calendar
Search
Planning travel Travel support Mileage Plus About United
earning points getting rewards
Great rewards!
new release DVDs
PROGRAMS & SERVICES
WORLDWIDE LOCATIONS
VEHICLE GUIDE
POLICIES & PROCEDURES
SPECIAL OFFERS
PARTNERSHIPS
ABOUT HERTZ
TRAVEL AGENTS
HERTZ HOME
Document: Done


BANKS
1st NAT'L:
jwayne412
iknowjohn
C.U.
johnwayne39
Pwd: 2Many Pwd
VISA
john_wayne32
pwd: spot1DØg$$
E- bay
user: johnwayne
pwd: john rules
Pay Pal
johnw93
KM34*
AMAZON
johnniew_41
Pwd: jwamazon
DELTA
johnw_d
pwd: flyme2
HOTMAIL
john_wayne942
pwd: spot My DØg
MASTERCARD
JW_1337
pwd: lol4u
B&N
jwayne_shop
Pwd: ibuystuff
SQL
sa:
Pwd: 3nØvA*9g
Messenger
johnwayne92
Pwd: jwmess92
EMAIL
user: jwayne
pwd: jwØ78T;
SlingPlayer_PC_1.4.0.206_Setup-US.exe
officeProdu...
Spin.exe
VistaDevPo...
buster_a...
Windows Installer
Preparing to install...
Cancel
Inbox - Microsoft O...
FY07Q4_MSDN_Eve...
Windows Media Pla...
Windows Installer

An Alternative (Web View)



● Round-trip ○ One-way ○ Multi-city

From: SEA

□ Add nearby airports custom

To:

□ Add nearby airports custom

My dates are flexible

Depart: 12/09/2011 Anytime

Fri, Dec 9 2011

Return: 12/14/2011 Anytime

Wed, Dec 14 2011

1 traveler

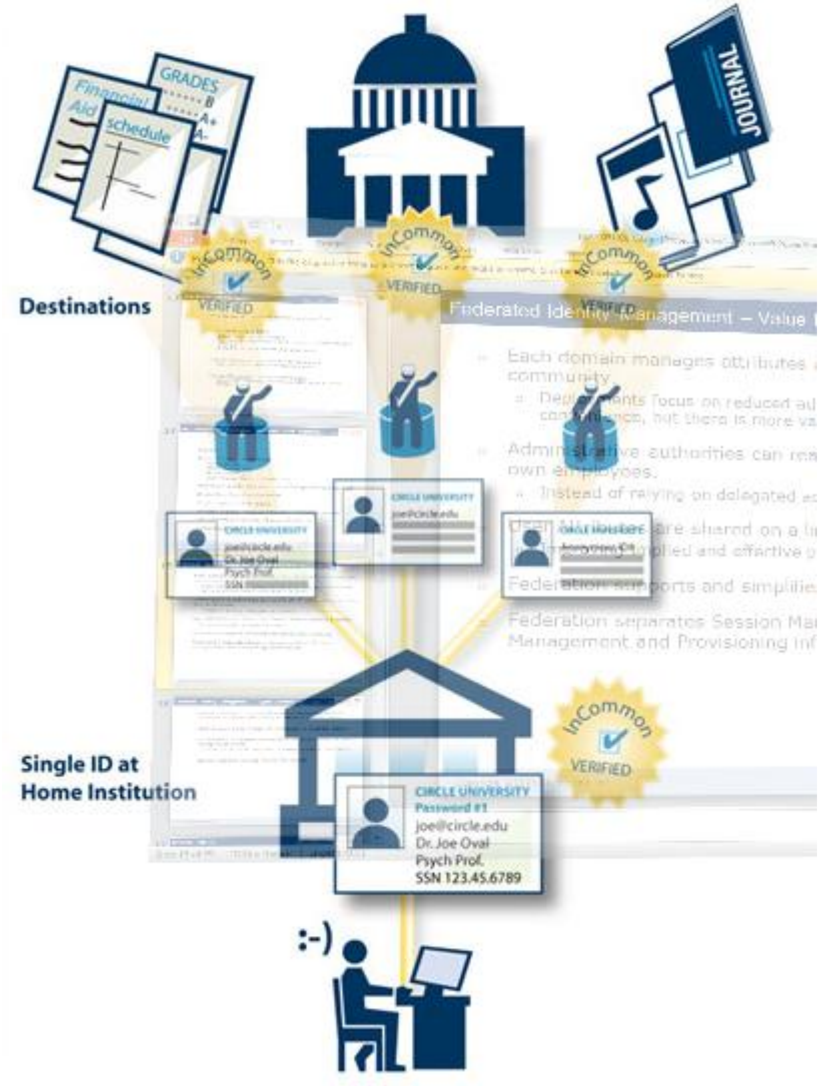
Economy

□ **Nonstops Only**

□ **Find Hotels** (in new window)

Compare hundreds of travel sites at once.

The Non-Web Scenario



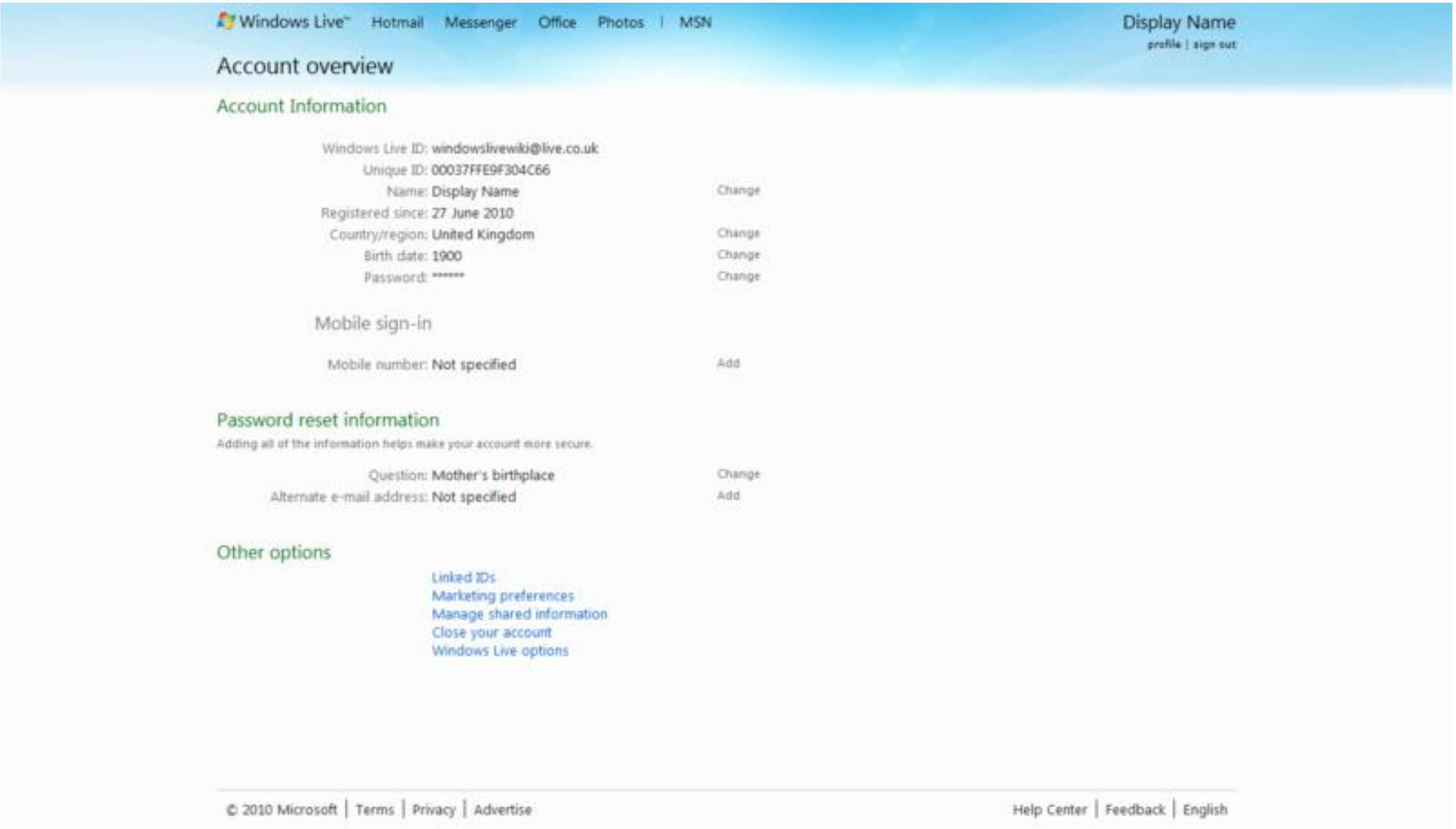
Push Toward Unified Identity Management

- Would like to maintain a single identity per user

- That identity act as user credentials for authentication and would be associated with extra user information
  - Name
  - Address
  - email,
  - etc.

- Gets us out of the situation where we have to remember dozens of login/password pairs

Editing User Identity Details



Account overview

Account Information

Windows Live ID: windowslivewiki@live.co.uk
Unique ID: 00037FFE9F304C66
Name: Display Name — Change
Registered since: 27 June 2010
Country/region: United Kingdom — Change
Birth date: 1900 — Change
Password: ****** — Change

Mobile sign-in

Mobile number: Not specified — Add

Password reset information

Adding all of the information helps make your account more secure.

Question: Mother's birthplace — Change
Alternate e-mail address: Not specified — Add

Other options

- Linked IDs
- Marketing preferences
- Manage shared information
- Close your account
- Windows Live options

© 2010 Microsoft | Terms | Privacy | Advertise
Help Center | Feedback | English

Overview: Federated Identity Model

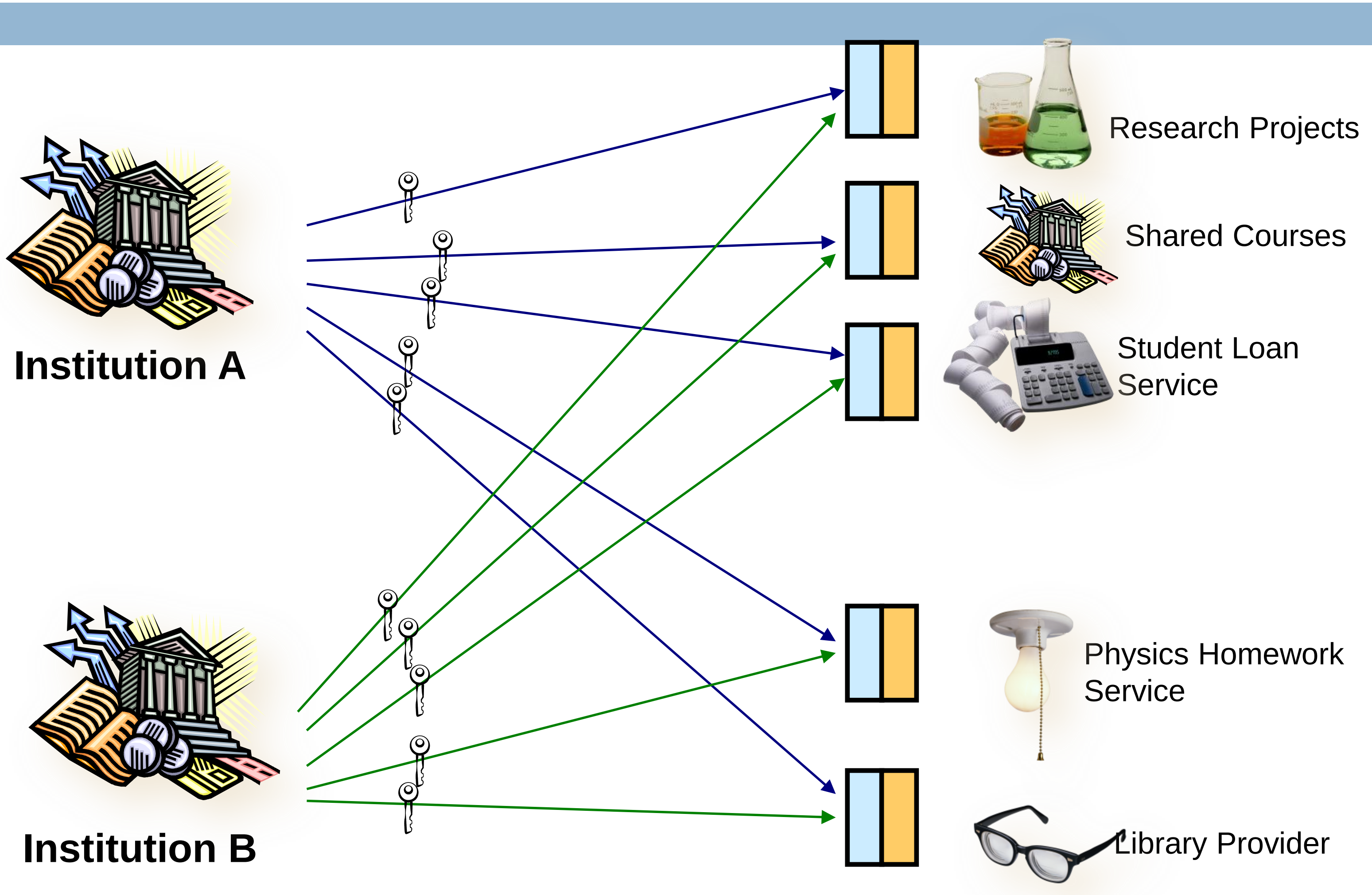
- The **user** is a person who assumes a particular digital identity to interact with an online network application

- The **user agent** is a browser or other software application that runs on anything from a PC to a mobile phone to a medical device. A user's online interactions always take place through an agent, which can passively allow identity information flow or actively mediate it

- The **service provider** (SP) site is a Web application— such as an expense-reporting application or an open source community—that offloads authentication to a third party, which might also send the SP some user attributes. Because the SP relies on external information, it's often called a relying party (RP)

- The **identity provider** (IdP) is a Web site that users log in to and that sometimes stores attributes of common interest to share with various SP

Traditional Identity Management



Research Projects

Shared Courses

Student Loan Service

Institution A

Physics Homework Service

Institution B

Library Provider

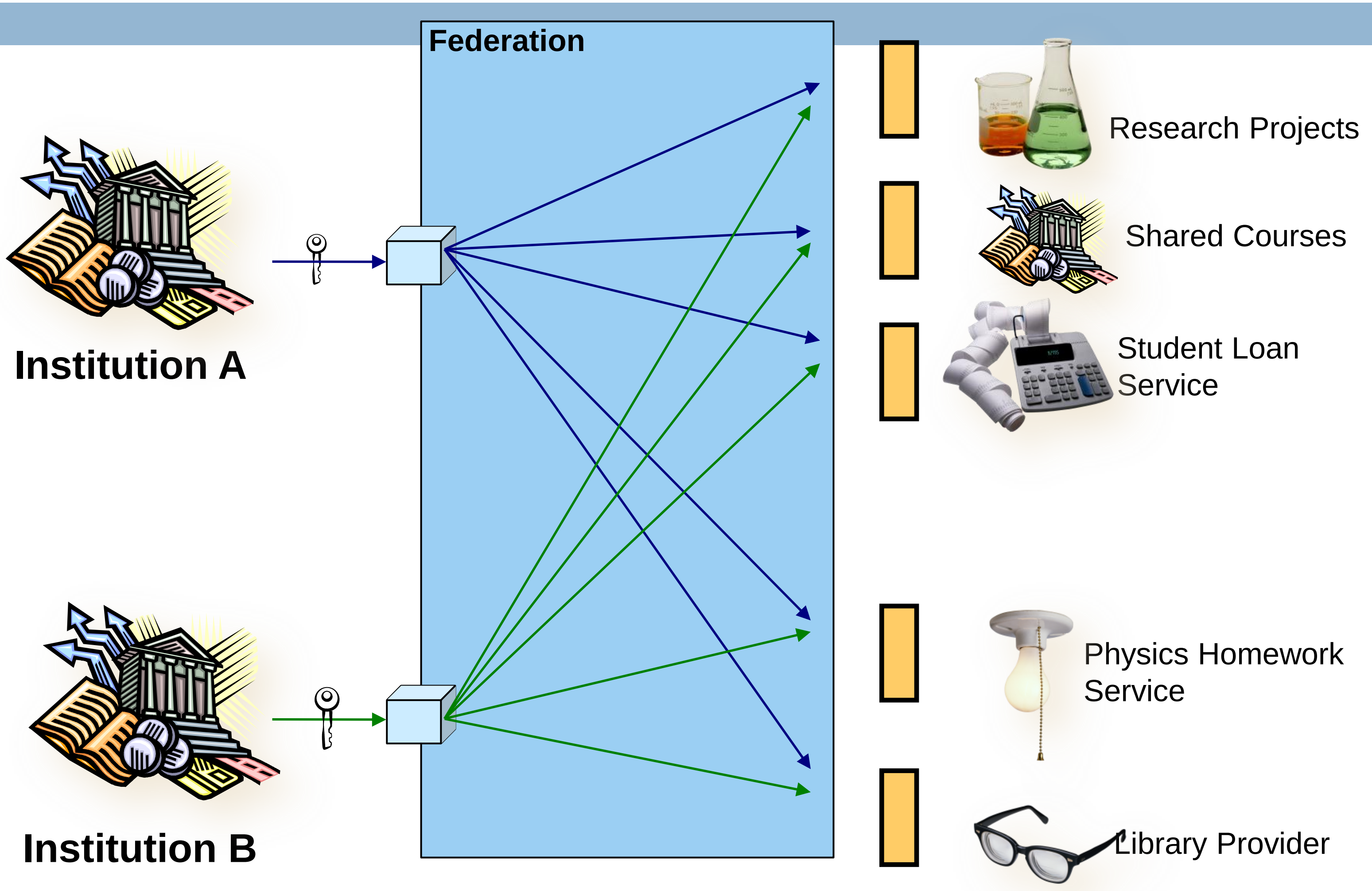
🟦 = Credentialing / Authentication

🟧 = Authorization

🔑 = User Credential

“Introduction to Federated Identity Management”, John O’Keefe

Federated Identity Concept



Federation

Institution A

Institution B

Research Projects

Shared Courses

Student Loan Service

Physics Homework Service

Library Provider

□ = Credentialing / Authentication

🟨 = Authorization

🔑 = User Credential

“Introduction to Federated Identity Management”, John O’Keefe

Example: InCommon Federation

- US Research and Education Federation
  - http://www.incommonfederation.org

- Over 200 participants representing over 4 million users and growing
  - Sponsored partners include the National Science Foundation, the TeraGrid, the National Institutes for Health, EDUCAUSE, the National Student Clearinghouse, and companies offering library databases, human resource systems, and other important services
  - Higher ed. participants include all types of colleges and universities – from the liberal arts to large research institutions

- Members agree to common participation rules and basic practices that allows each to inter-operate with the others

“Introduction to Federated Identity Management”, John O’Keefe

SP-Initiated SSO

- Alice begins her browsing at an SP, such as an investment management site, which she might visit frequently

- Alice wants to access protected resources there, the SP must send an explicit authentication request to Alice's bank (the IdP)

IdP-Initiated SSO

- IdP, such as a health insurance site, acts as a portal through which Alice accesses various SPs, such as online pharmacies and billing statement aggregators

- In either case, if Alice’s relationship with an SP predates her IdP relationship, the IdP and the SP accounts must be linked (with her permission) to make SSO successful

Identity and its Usage is Separate

- Alice can log in once—with one set of credentials—and access multiple Web sites without revealing her credentials to all of them

- SPs can delegate many account-management tasks (such as password resets) and receive accurate just-in-time user data

- IdPs can focus on improving authentication methods and adding attractive features to account management interfaces

Privacy Considerations

- Basic challenge
  - Need to ensure that SPs don’t learn more about the user than absolutely necessary

- Pseudonyms is what’s often used
- However, two basic challenges remain
  - Extra information added to the pseudonym such as postcodes and gender and income can be used to deanonymize the user
  - Multiple SPs can collude and put their information about the user with the same pseudonym together, thereby recovering more information

Deanonymization Attacks

- What Information is **personally Identifiable**?
- Mr. X lives in ZIP code 02138 and was born July 31, 1945
- These facts about him were included in an anonymized medical record released to the public

- Sounds like Mr. X is pretty anonymous, right?
- Latanya Sweeney, a Carnegie Mellon University computer science professor showed in 1997 that this information was enough to pin down Mr. X's more familiar identity -- William Weld, the governor of Massachusetts throughout the 1990s

PII or Not?

- Gender, ZIP code, and birth date feel anonymous, but Prof. Sweeney was able to identify Governor Weld through them for two reasons
- First, each of these facts about an individual (or other kinds of facts we might not usually think of as identifying) independently narrows down the population, so much so that the combination of (gender, ZIP code, birthdate) was unique for about 87% of the U.S. population
- If you live in the United States, there's an 87% chance that you don't share all three of these attributes with any other U.S. resident
- Second, there may be particular data sources available (Sweeney used a Massachusetts voter registration database) that let people do searches to bootstrap what they know about someone in order to learn more -- including traditional identifiers like name and address.
- In a very concrete sense, "anonymized" or "merely demographic" information about people may be neither.
- (And a web site that asks "anonymous" users for seemingly trivial information about themselves may be able to use that information to make a unique profile for an individual, or even look up that individual in other databases.)

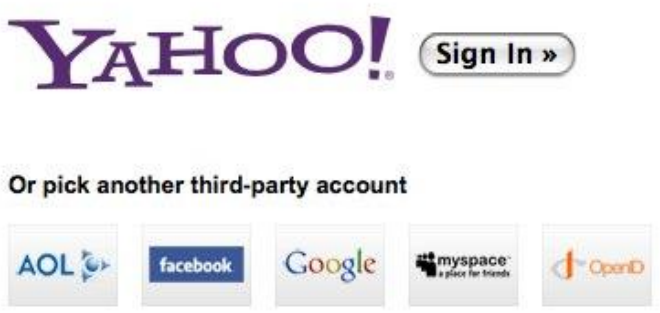
Architectural Challenges of SSO

- IdP discovery
  - When an SP wants to initial a logon, which IdP do they send the user to?
  - SPs can be bound to a particular IdP
  - Can provide the user with a choice of identity providers

  - Or have the user agent decide

  which identity to use:

  think Android of Facebook phone



Or pick another third-party account

User Empowerment

- Focus on user-centric identity
- Give users control about what information is associated with their identity

- Privacy:
  - Prompt users and require involvement in sharing decisions

- Integrity:
  - Information about users is not necessarily verified by anyone else, so users can claim to be whoever they want to be

"On the Internet, nobody knows you're a dog."

Popular Identity Protocols

- SAML
- OpenID
- InfoCard/CardSpace

Question of the Day

Would it make sense for a government entity to be an identity provider?

NSTIC: National Strategy for Trusted Identities in Cyberspace

About NSTIC

The National Strategy for Trusted Identities in Cyberspace (NSTIC) is a White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions.

The Strategy calls for the development of interoperable technology standards and policies — an"Identity Ecosystem" — where individuals, organizations, and underlying infrastructure — such as routers and servers — can be authoritatively authenticated. The goals of the Strategy are to protect individuals, businesses, and public agencies from the high costs of cyber crimes like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas.

SAML: SAML Assertions

- An assertion contains a packet of security information:

  ```
  <saml:Assertion …>
    …
  </saml:Assertion>
  ```

- How to interpret the assertion:
  Assertion *A* was issued at time *t* by issuer *R* subject to conditions *C*

Assertion Example

- A typical SAML 1.1 assertion:

```
<saml:Assertion
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  MajorVersion="1" MinorVersion="1"
  AssertionID="a75adf55-01d7-40cc-929f-dbd8372ebdfc"
  IssueInstant="2004-12-05T09:22:02Z"
  Issuer="https://idp.example.org/saml">
  <saml:Conditions
    NotBefore="2004-12-05T09:17:02Z"
    NotOnOrAfter="2004-12-05T09:27:02Z"/>
  <!-- insert statement here -->
</saml:Assertion>
```

- The value of the `Issuer` attribute is the unique identifier of the SAML authority

SAML Statements

- SAML assertions contain statements

- Three types of SAML statements:
  1. Authentication statements
  2. Attribute statements
  3. Authorization decision statements

- Although statements are the “meat” of assertions, the assertion remains the atomic unit of SAML

Authentication Statement

- A typical *authentication statement* asserts: Subject *S* authenticated at time *t* using authentication method *m*
- A `NameIdentifier` refers to subject *S*
- The `NameIdentifier` has properties:
  - transparent or opaque
  - persistent or transient

SAML Subject

- □ In a statement, the SAML Subject is crucial:

```
<saml:Subject

xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
<saml:NameIdentifier

Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"

NameQualifier="https://idp.example.org/saml">

    user@example.org

  </saml:NameIdentifier>
  …
</saml:Subject>
```

- □ In this example, the Format of the NameIdentifier is an emailAddress, a transparent, persistent identifier
- □ In deployments where privacy is an issue, an opaque, transient identifier is more appropriate
- □ Unfortunately, SAML 1.1 does not specify such an identifier (but SAML 2.0 does)

Statement Example

- A subject-based authentication statement:

```
<saml:AuthenticationStatement
  xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
  AuthenticationInstant="2004-12-05T09:22:00Z"
  AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
  <saml:Subject>
    <saml:NameIdentifier
      Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName"
      NameQualifier="https://idp.ncsa.uiuc.edu/saml">
      CN=GridShib,OU=NCSA,O=UIUC
    </saml:NameIdentifier>
  </saml:Subject>
</saml:AuthenticationStatement>
```

- In this example, we use an X.509 subject DN as a `NameIdentifier`
- Note also the time and method of authentication

Shibboleth

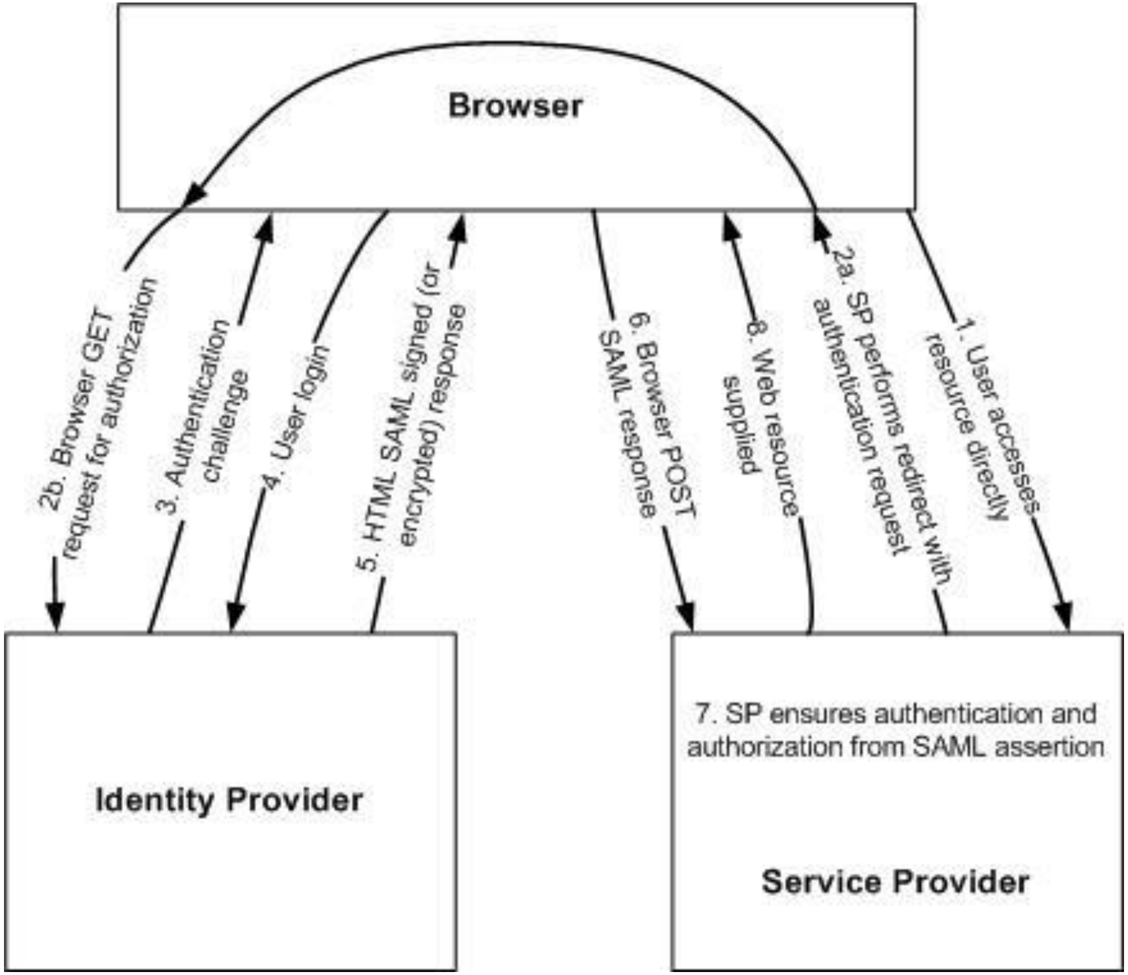
- First large-scale Federated Security solution
- Secures web sites and web applications
- Implements Security Assertion Markup Language (SAML) standard

- Initially developed for research and higher education
  - Research collaboration
  - Academic information providers
  - Outsourced employee applications
  - Extended user populations
- Open source project

Security Assertions

- Attributes assigned to user accounts
- Represent group affiliation or user privilege
  - No predefined semantics by Shibboleth
  - Semantic agreement among participants
  - Federation and two-party arrangements
- Bundled with resource requests
  - Authenticated by IdP
  - Basis of resource authorization by SP

Shibboleth Web Application SSO


Browser
2b. Browser GET request for authorization
3. Authentication challenge
4. User login
5. HTML SAML signed (or encrypted) response
6. Browser POST SAML response
8. Web resource supplied
2a. SP performs redirect with authentication request
1. User accesses resource directly
Identity Provider
7. SP ensures authentication and authorization from SAML assertion
Service Provider

Source: "Web Single Sign-On Authentication using SAML"

Web Application SSO Details

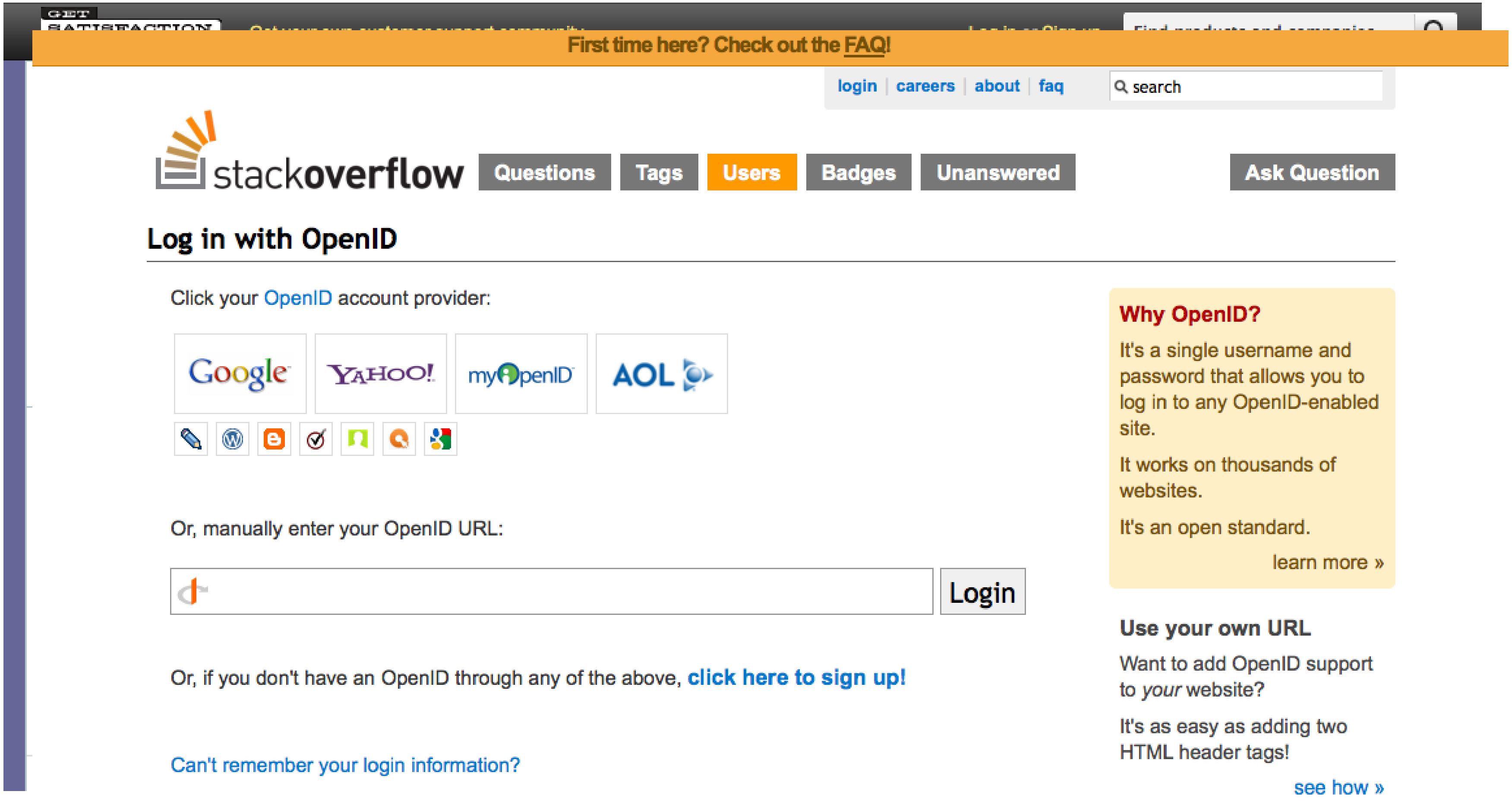
- Based on SAML Web Browser SSO Profile
- Standard browser request, e.g. GET
- Where-Are-You-From service locates IdP
- User browser redirected to IdP
  - Automated with JavaScript or manually invoked
- IdP specific identity verification
- Digitally signed security assertions
- Browser session enables single sign-on

OpenID

What is OpenID

- URL
  - Unique to user
  - User can claim
  - Use for authentication
- Single-Sign On
- Decentralized: URL can reside in any domain
- Anonymous: URLs (pseudonyms) are used

OpenID In Use



First time here? Check out the FAQ!

Log in with OpenID

Click your OpenID account provider:

Or, manually enter your OpenID URL:

Or, if you don't have an OpenID through any of the above, **click here to sign up!**

Can't remember your login information?

Why OpenID?

It's a single username and password that allows you to log in to any OpenID-enabled site.

It works on thousands of websites.

It's an open standard.

learn more »

Use your own URL

Want to add OpenID support to *your* website?

It's as easy as adding two HTML header tags!

see how »

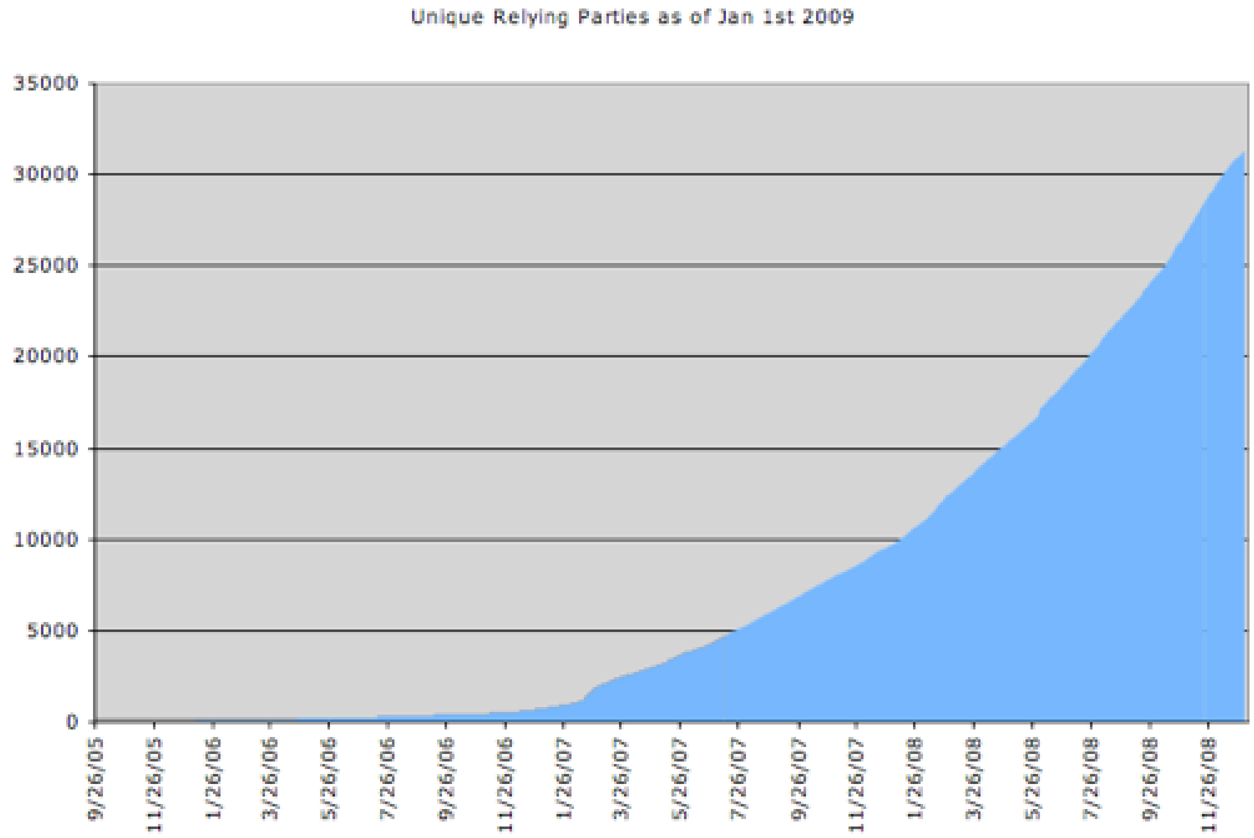
OpenID History

- May 2005 – OpenID authentication protocol developed by Brad Fitzpatrick
- May 2006 – JanRain developed Simple Registration Extension (profile-exchange)
- May 2006 – Incorporate XRI support
- Jan 2007 – Symantic supports OpenID

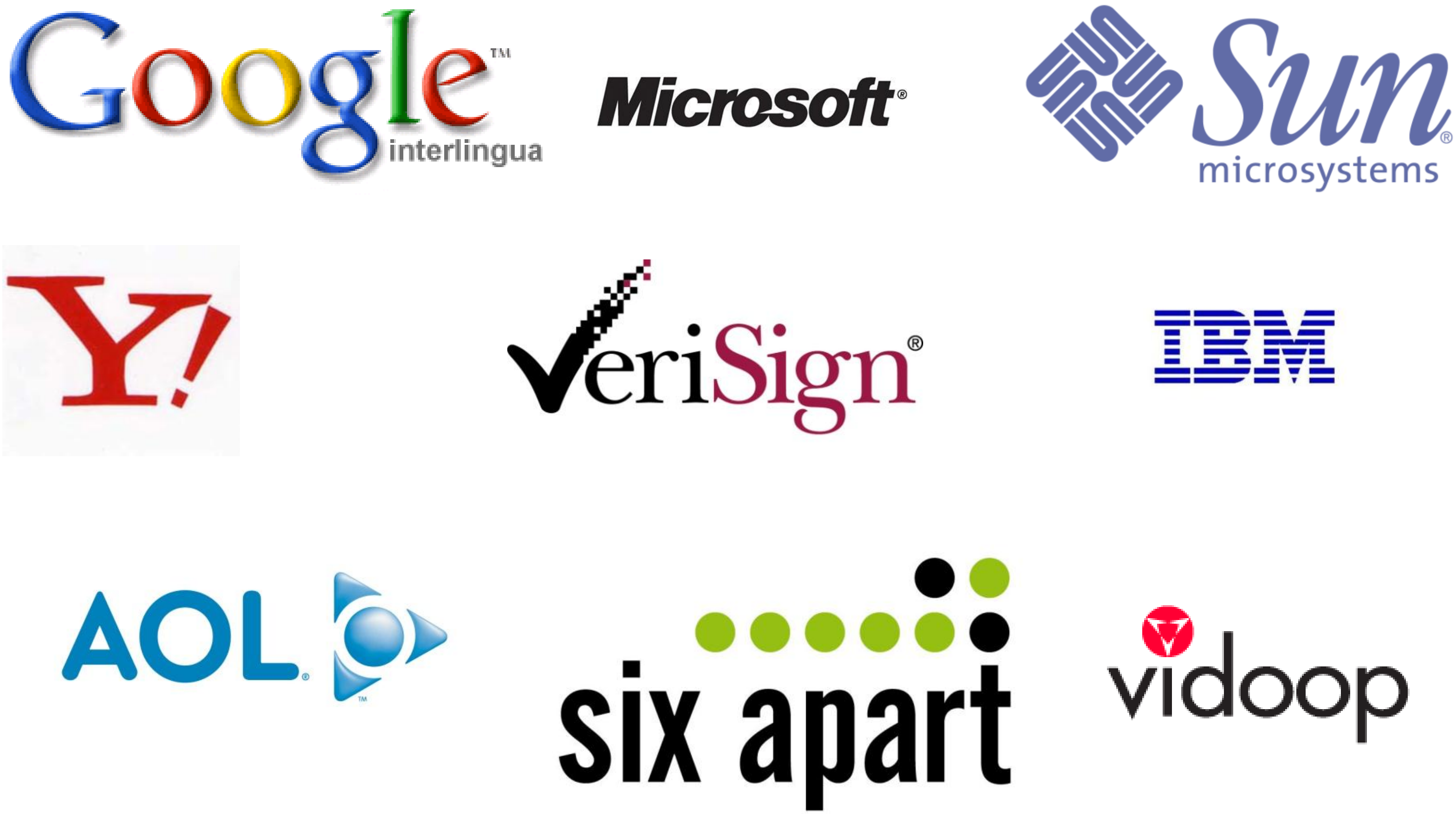
OpenID History

- Feb 2007 – Microsoft, AOL supports OpenID
- May 2007 – Sun Microsystem supports OpenID
- June 2007 – OpenID Foundation formed in Oregon
- Jan 2008 – Yahoo! Supports OpenID
- Feb 2008 – Google, IBM, VeriSign, and Yahoo joined OpenID Foundation corporate board
- In January 2009, PayPal joined the OpenID Foundation as a corporate member, followed shortly by Facebook in February

Sites Supporting OpenID



Key Adopters



How OpenID Works

RP – Relaying Party: OpenID Supported Page

OP – OpenID Provider: such as livejournal.com or aol.com

1. User initiates authentication process
2. RP Perform Discover/Normalize identifier
3. Establish an Association (Diffie-Hellman Key Exchange)
4. RP directions User to OP with request
5. OP Authorizes/Deny request
6. OP redirects User to RP with authorization approved/denied
7. RP verifies information + OP sources

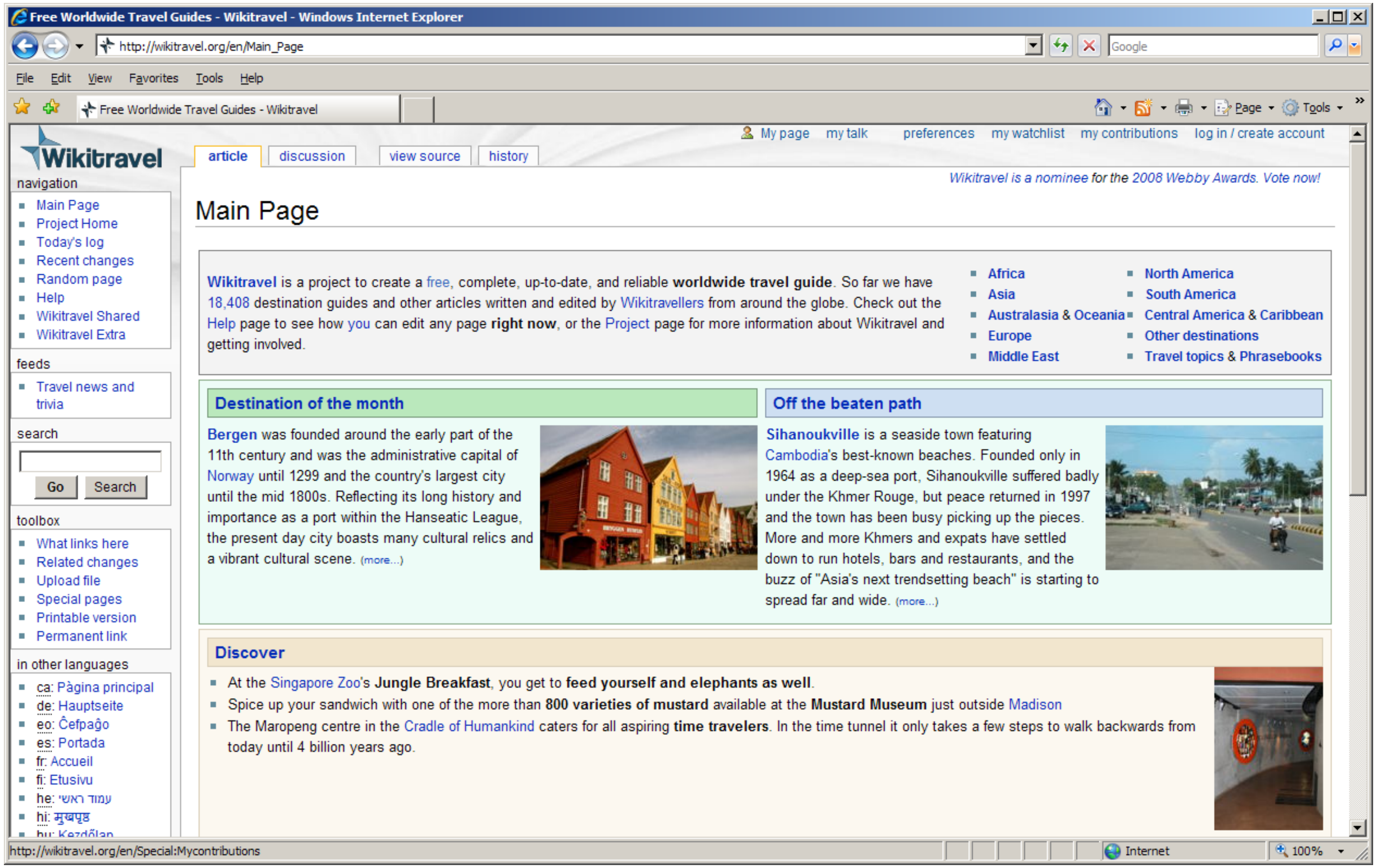
Self-Hosting an OpenID

```
 <link rel="openid.server"
        href="http://www.myopenid.com/server" />
  <link rel="openid.delegate"
        href="http://youraccount.myopenid.com/" />
  <link rel="openid2.local_id"
        href="http://youraccount.myopenid.com" />
  <link rel="openid2.provider"
        href="http://www.myopenid.com/server" />
  <meta http-equiv="X-XRDS-Location"

content="http://www.myopenid.com/xrds?username=youraccoun
t.myopenid.com" />
```

OpenID Scenario (1)

Enter OpenID Supported Page (Relaying Party)



Wikitravel is a nominee for the 2008 Webby Awards. Vote now!

Main Page

Wikitravel is a project to create a free, complete, up-to-date, and reliable **worldwide travel guide**. So far we have 18,408 destination guides and other articles written and edited by Wikitravellers from around the globe. Check out the Help page to see how you can edit any page **right now**, or the Project page for more information about Wikitravel and getting involved.

Destination of the month

Bergen was founded around the early part of the 11th century and was the administrative capital of Norway until 1299 and the country's largest city until the mid 1800s. Reflecting its long history and importance as a port within the Hanseatic League, the present day city boasts many cultural relics and a vibrant cultural scene. (more...)

Off the beaten path

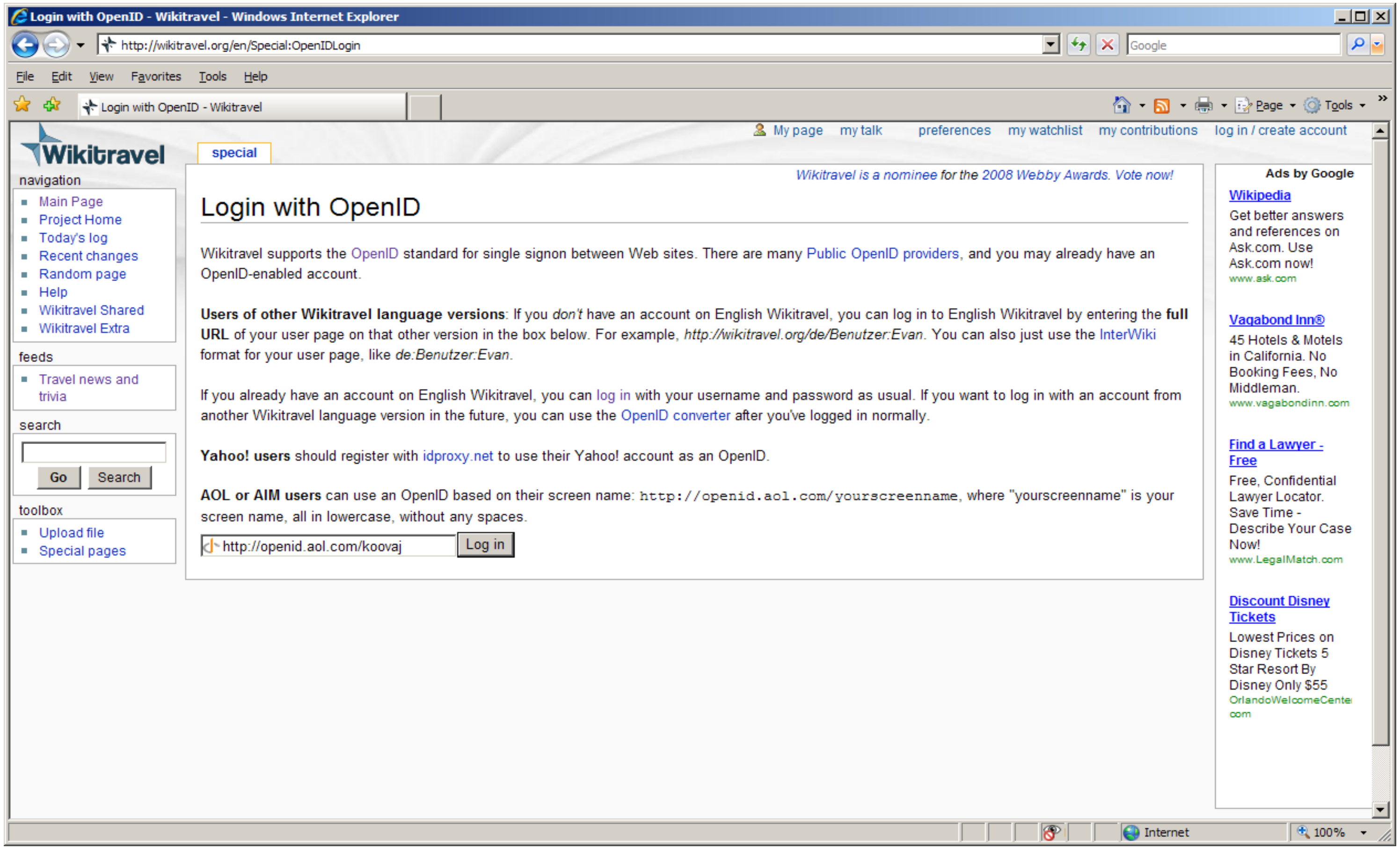
Sihanoukville is a seaside town featuring Cambodia's best-known beaches. Founded only in 1964 as a deep-sea port, Sihanoukville suffered badly under the Khmer Rouge, but peace returned in 1997 and the town has been busy picking up the pieces. More and more Khmers and expats have settled down to run hotels, bars and restaurants, and the buzz of "Asia's next trendsetting beach" is starting to spread far and wide. (more...)

Discover

- At the Singapore Zoo's **Jungle Breakfast**, you get to **feed yourself and elephants as well**.
- Spice up your sandwich with one of the more than **800 varieties of mustard** available at the **Mustard Museum** just outside Madison
- The Maropeng centre in the Cradle of Humankind caters for all aspiring **time travelers**. In the time tunnel it only takes a few steps to walk backwards from today until 4 billion years ago.

OpenID Scenario (2)

- OpenID Login (http://openid.aol.com/koovaj)


Login with OpenID - Wikitravel - Windows Internet Explorer
http://wikitravel.org/en/Special:OpenIDLogin
Google
File Edit View Favorites Tools Help
Login with OpenID - Wikitravel
Page Tools
My page my talk preferences my watchlist my contributions log in / create account
Wikitravel
special
navigation
Main Page
Project Home
Today's log
Recent changes
Random page
Help
Wikitravel Shared
Wikitravel Extra
feeds
Travel news and trivia
search
Go Search
toolbox
Upload file
Special pages
Internet
100%

Wikitravel is a nominee for the 2008 Webby Awards. Vote now!

Login with OpenID

Wikitravel supports the OpenID standard for single signon between Web sites. There are many Public OpenID providers, and you may already have an OpenID-enabled account.

Users of other Wikitravel language versions: If you *don't* have an account on English Wikitravel, you can log in to English Wikitravel by entering the **full URL** of your user page on that other version in the box below. For example, *http://wikitravel.org/de/Benutzer:Evan*. You can also just use the InterWiki format for your user page, like *de:Benutzer:Evan*.

If you already have an account on English Wikitravel, you can log in with your username and password as usual. If you want to log in with an account from another Wikitravel language version in the future, you can use the OpenID converter after you've logged in normally.

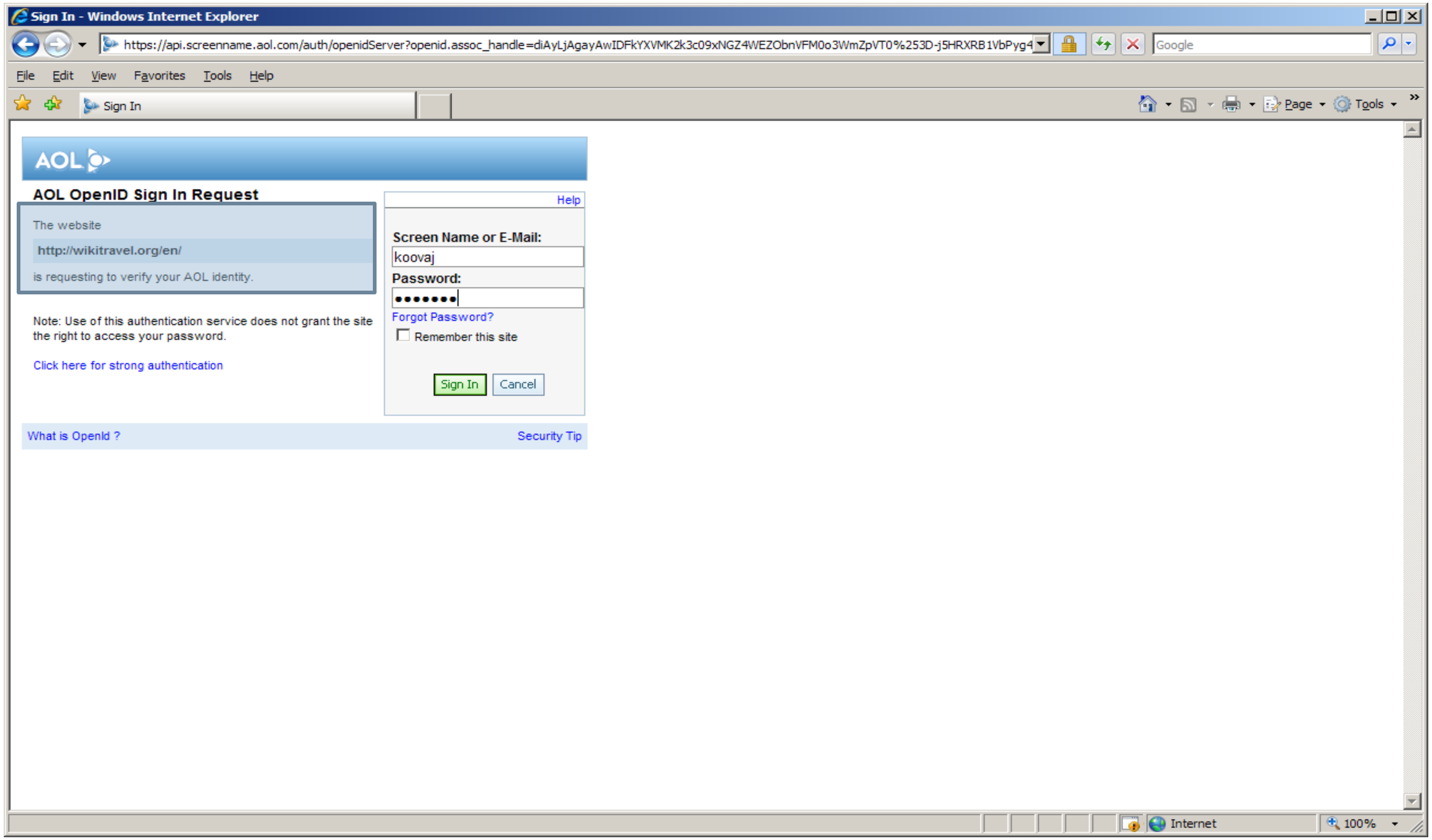
Yahoo! users should register with idproxy.net to use their Yahoo! account as an OpenID.

AOL or AIM users can use an OpenID based on their screen name: `http://openid.aol.com/yourscreenname`, where "yourscreenname" is your screen name, all in lowercase, without any spaces.

http://openid.aol.com/koovaj [Log in]

OpenID Scenario (3)

- Redirected to OpenID Provider for auth



Sign In - Windows Internet Explorer
https://api.screenname.aol.com/auth/openidServer?openid.assoc_handle=diAyLjAgayAwIDFkYXVMK2k3c09xNGZ4WEZObnVFM0o3WmZpVT0%253D-j5HRXRB1VbPyg4
Google
File
Edit
View
Favorites
Tools
Help
Sign In
Page
Tools
AOL
Internet
100%

AOL OpenID Sign In Request

The website

http://wikitravel.org/en/

is requesting to verify your AOL identity.

Note: Use of this authentication service does not grant the site the right to access your password.

Click here for strong authentication

Help

Screen Name or E-Mail: koovaj

Password: •••••••

Forgot Password?

□ Remember this site

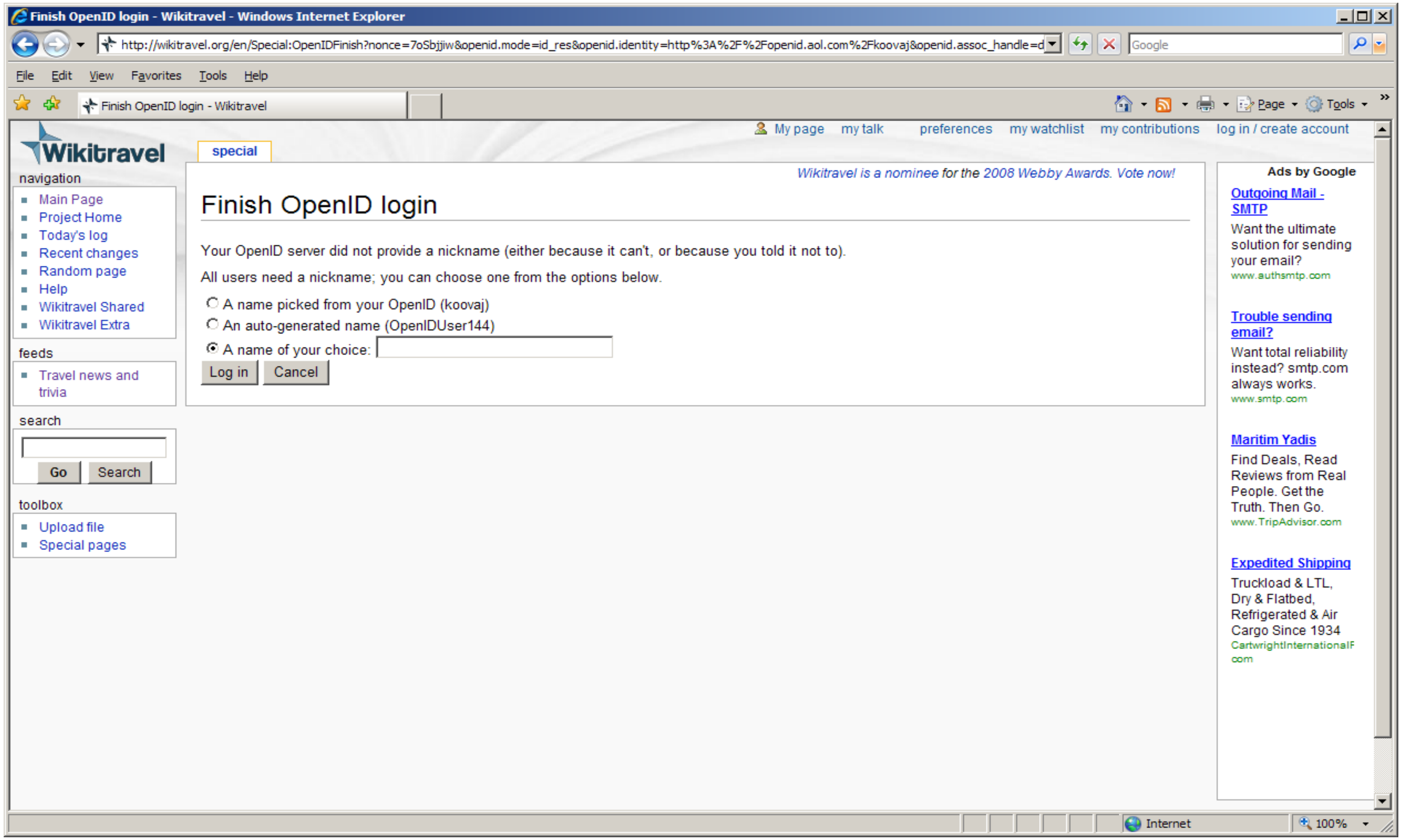
Sign In | Cancel

What is OpenId ?

Security Tip

OpenID Scenario (4)

- Redirect to Relaying Party (granted/denied)


Finish OpenID login - Wikitravel - Windows Internet Explorer
http://wikitravel.org/en/Special:OpenIDFinish?nonce=7oSbjjiw&openid.mode=id_res&openid.identity=http%3A%2F%2Fopenid.aol.com%2Fkoovaj&openid.assoc_handle=d
Google
File Edit View Favorites Tools Help
Finish OpenID login - Wikitravel
Page Tools
My page my talk preferences my watchlist my contributions log in / create account
Wikitravel
special
navigation
Main Page
Project Home
Today's log
Recent changes
Random page
Help
Wikitravel Shared
Wikitravel Extra
feeds
Travel news and trivia
search
Go Search
toolbox
Upload file
Special pages
Wikitravel is a nominee for the 2008 Webby Awards. Vote now!
Ads by Google
Outgoing Mail - SMTP
Want the ultimate solution for sending your email?
www.authsmtp.com
Trouble sending email?
Want total reliability instead? smtp.com always works.
www.smtp.com
Maritim Yadis
Find Deals, Read Reviews from Real People. Get the Truth. Then Go.
www.TripAdvisor.com
Expedited Shipping
Truckload & LTL, Dry & Flatbed, Refrigerated & Air Cargo Since 1934
CartwrightInternationalF com
Internet
100%

Finish OpenID login

Your OpenID server did not provide a nickname (either because it can't, or because you told it not to).

All users need a nickname; you can choose one from the options below.

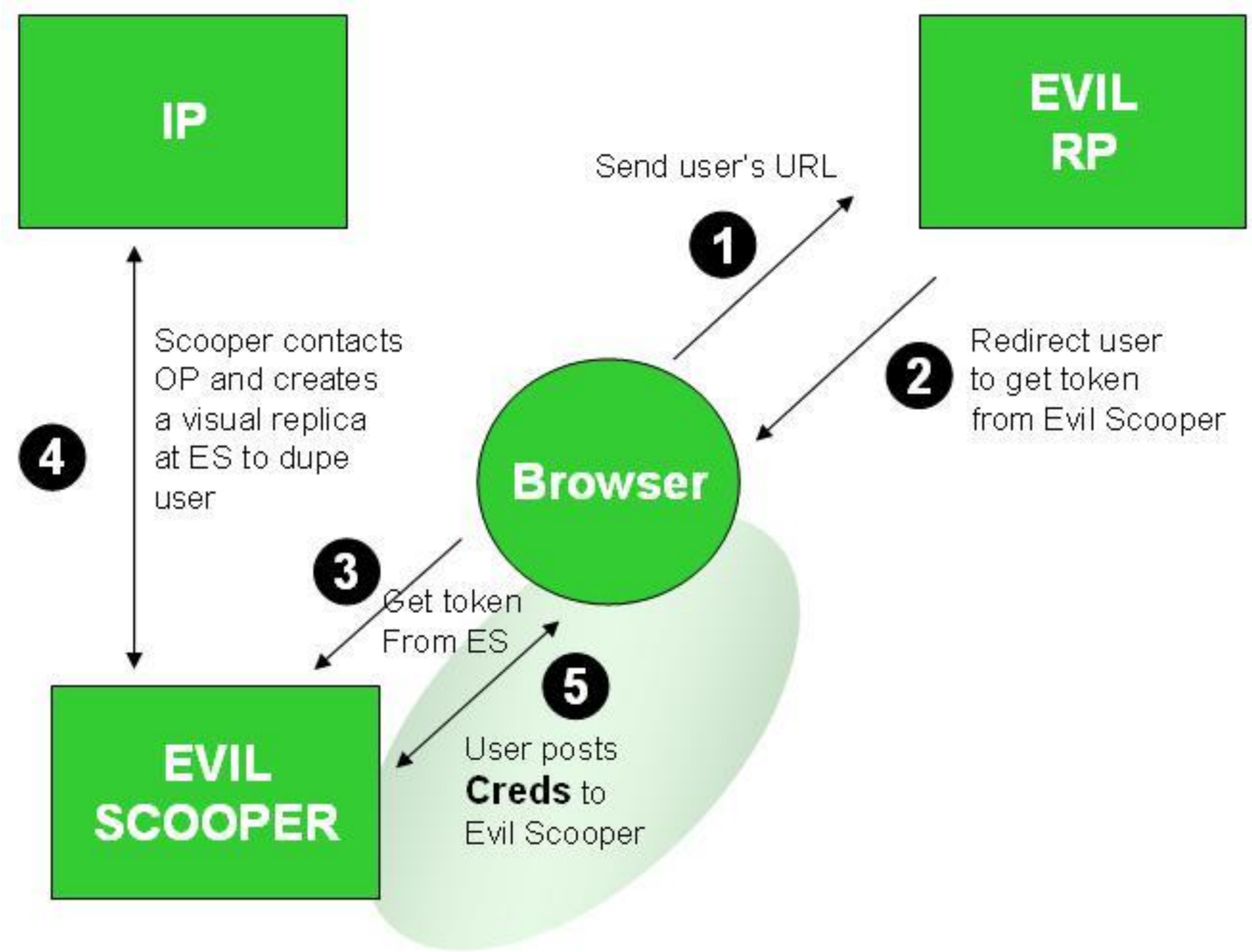
○ A name picked from your OpenID (koovaj)

○ An auto-generated name (OpenIDUser144)

● A name of your choice:

Log in | Cancel

Phishing is a Challenge


IP
EVIL RP
Send user's URL
1
2
Redirect user to get token from Evil Scooper
4
Scooper contacts OP and creates a visual replica at ES to dupe user
Browser
3
Get token From ES
5
User posts **Creds** to Evil Scooper
EVIL SCOOPER

MS Passport: Fake Merchant Attack

- Same as phishing issues we saw before
  - Bob = Passport user
  - Mallory = Attacker of Malicious party

- **Assumption**: Bob get accustomed to using passport and trust the security of the passport server

How to Attack?

1. Mallory sets up a phony web

2. Mallory gets a certificate for a web site, called pasport.com. And Mallory sets up his web site which is exactly the same as a real passport.com.

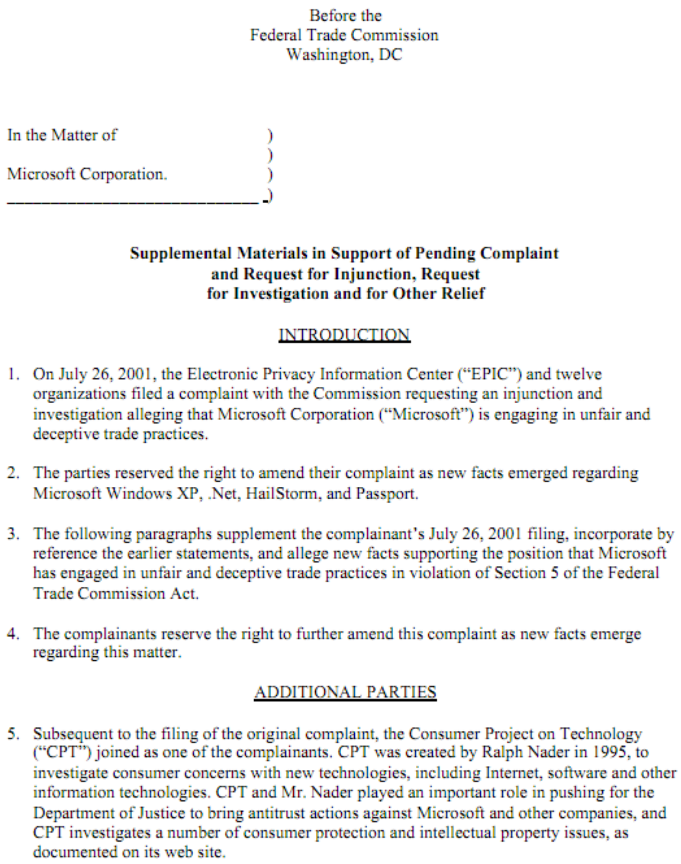
3. So Bob want to buy something in Mallory's shop, click sign-in, the server creates a redirect to Mallory's pasport.com. Bob is in the habit of filling his Email Address and Password

4. After that, Mallory has got Bob's valid authentication information, and he can go to online shop, use Bob's wallet service on behalf of Bob

Attacks on MS Passport

- □ Fake merchant attack
- □ DNS poisoning attack
- □ Client-side Cookie-based attack

Microsoft .net Passport



Before the
Federal Trade Commission
Washington, DC

In the Matter of)
)
Microsoft Corporation.)
____________________________)

**Supplemental Materials in Support of Pending Complaint
and Request for Injunction, Request
for Investigation and for Other Relief**

INTRODUCTION

1. On July 26, 2001, the Electronic Privacy Information Center ("EPIC") and twelve organizations filed a complaint with the Commission requesting an injunction and investigation alleging that Microsoft Corporation ("Microsoft") is engaging in unfair and deceptive trade practices.

2. The parties reserved the right to amend their complaint as new facts emerged regarding Microsoft Windows XP, .Net, HailStorm, and Passport.

3. The following paragraphs supplement the complainant's July 26, 2001 filing, incorporate by reference the earlier statements, and allege new facts supporting the position that Microsoft has engaged in unfair and deceptive trade practices in violation of Section 5 of the Federal Trade Commission Act.

4. The complainants reserve the right to further amend this complaint as new facts emerge regarding this matter.

ADDITIONAL PARTIES

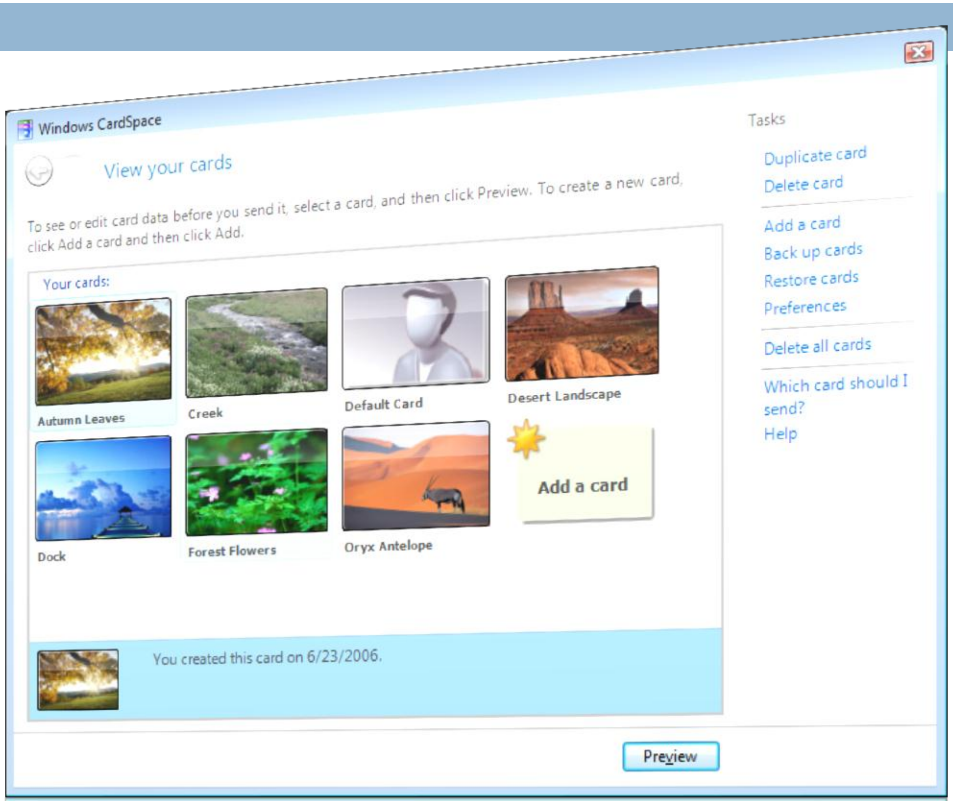
5. Subsequent to the filing of the original complaint, the Consumer Project on Technology ("CPT") joined as one of the complainants. CPT was created by Ralph Nader in 1995, to investigate consumer concerns with new technologies, including Internet, software and other information technologies. CPT and Mr. Nader played an important role in pushing for the Department of Justice to bring antitrust actions against Microsoft and other companies, and CPT investigates a number of consumer protection and intellectual property issues, as documented on its web site.

Windows CardSpace

- Windows CardSpace is a piece of client software that enables users to provide their digital identity to online services in a simple, secure and trusted way

CardSpace Environment

- □ Runs under separate desktop and restricted account
- □ Isolates CardSpace runtime from Windows desktop
- □ Deters hacking attempts by user-mode processes



To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

You created this card on 6/23/2006.

CardSpace Cards

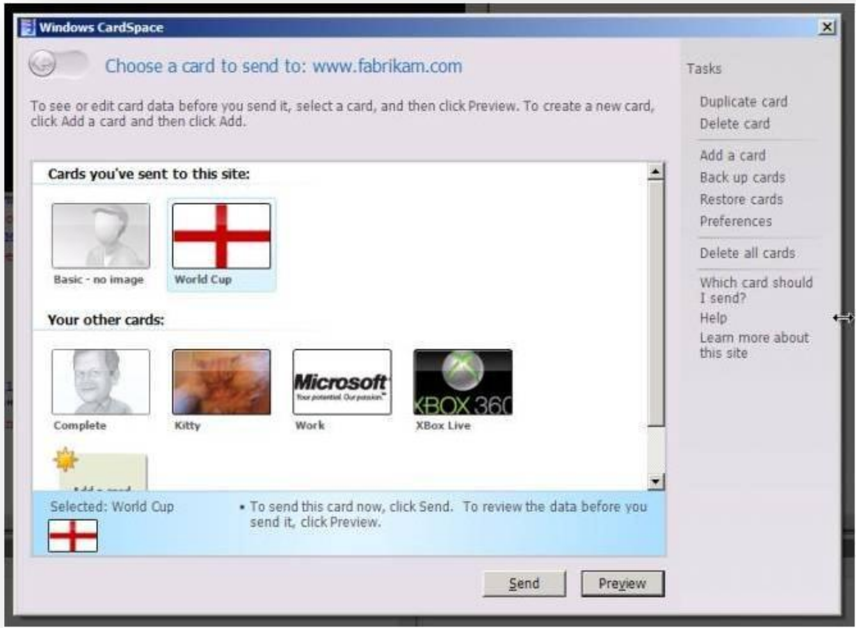
- Contains claims about my identity that I assert
- Not corroborated
- Stored locally
- Signed and encrypted to prevent replay attacks

- Provided by banks, stores, government, clubs, etc
- Locally stored cards contain metadata only!
- Data stored by Identity Provider and obtained only when card submitted
- Users can’t edit claims
- Can be protected by various means (Username/Password, Kerberos, SmartCard etc)

The Identity Selector

Easier:
No usernames
No passwords

Consistent:
Same UI


Choose a card to send to: www.fabrikam.com

To see or edit card data before you send it, select a card, and then click Preview. To create a new card, click Add a card and then click Add.

Cards you've sent to this site:

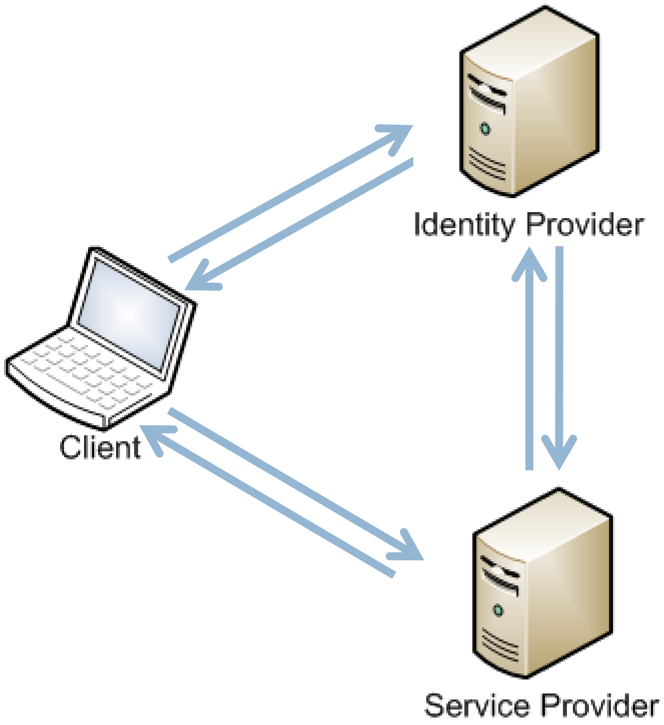
Your other cards:

Selected: World Cup

- To send this card now, click Send. To review the data before you send it, click Preview.

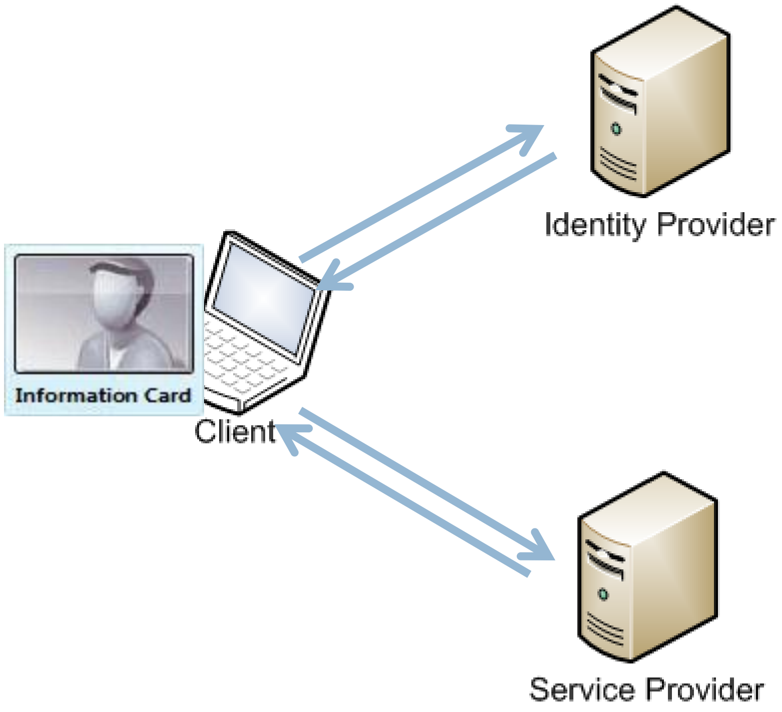
Safer:
Avoids Phishing
Multi-factor
authentication

The Typical Logon Process



1. Login to identity provider
2. Token issued to client
3. Token sent to service provider
4. Token validated with identity provider
5. Output sent to client

The CardSpace Logon Process



1. Service Provider Requests Identity
2. CardSpace Identity Selector pops up
3. Token is built by Identity Selector (with Identity Provider)
4. Token sent to client
5. Output sent to client

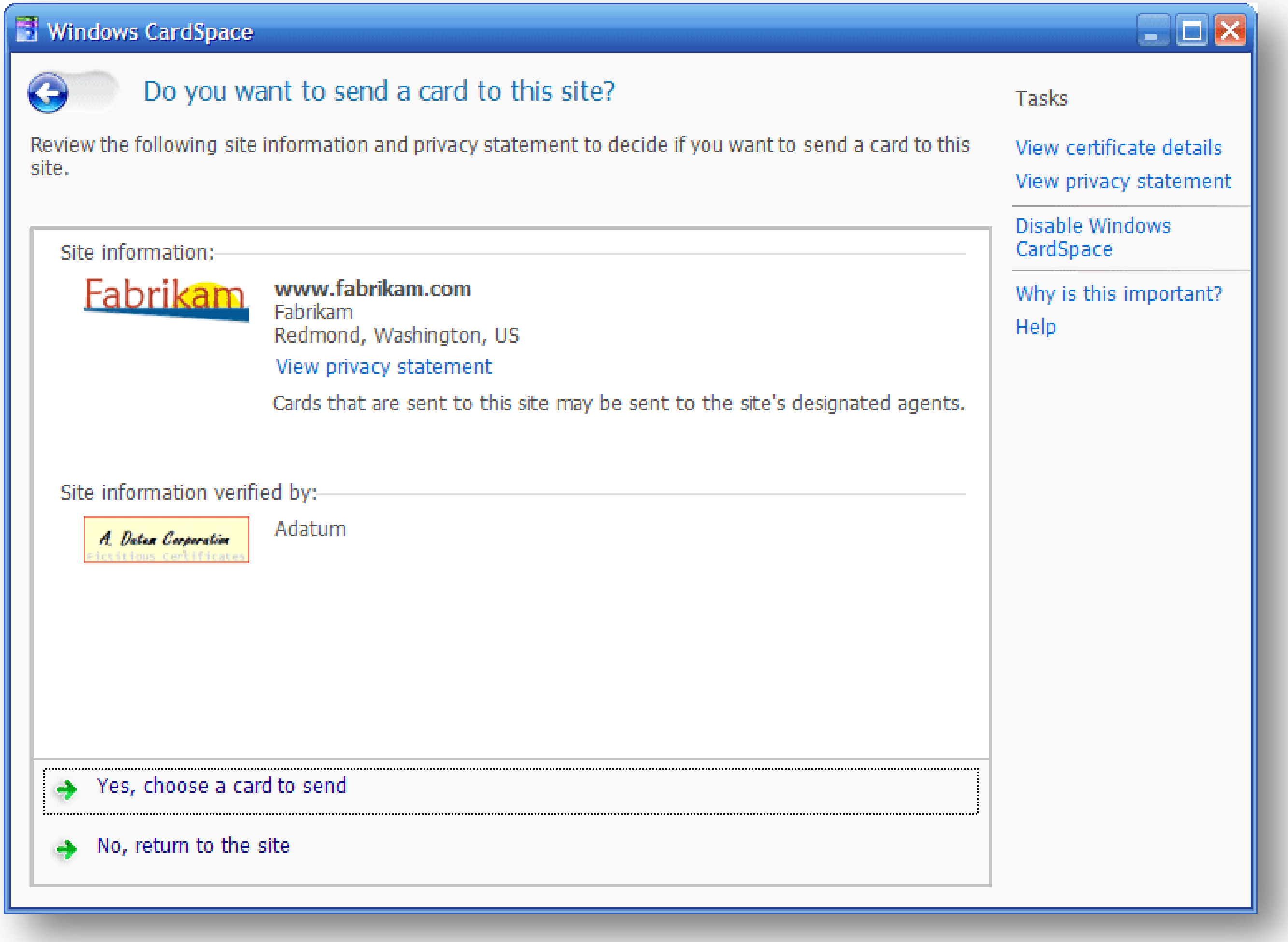
CardSpace Versus OpenID/Passport

Cardspace	Open ID
Client side prompt (IE support/FireFox community code)	HTML Form
Common User Experience	Experience varies between Identity Providers
Simpler Login	Redirection / Site Bounce
Requires EV SSL	No SSL required

Requesting a CardSpace InfoCard

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
  <title>Sample 1</title>
</head>
<body>
    <form id="form1" method="post" action="login1.aspx">
      <button type="submit">Click here to sign in with your Information Card</button>
      <object type="application/x-informationcard" name="xmlToken">
        <param name="tokenType" value="urn:oasis:names:tc:SAML:1.0:assertion" />
        <param name="issuer"
               value="http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self" />
        <param name="requiredClaims"
             value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
                    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname
                    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
                    http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier" />
      </object>
    </form>
</body>
</html>
```

CardSpace Identity Selector



Windows CardSpace

Do you want to send a card to this site?

Review the following site information and privacy statement to decide if you want to send a card to this site.

Site information:

Fabrikam

www.fabrikam.com
Fabrikam
Redmond, Washington, US
View privacy statement

Cards that are sent to this site may be sent to the site's designated agents.

Site information verified by:

A. Datum Corporation
Fictitious Certificates

Adatum

Yes, choose a card to send

No, return to the site

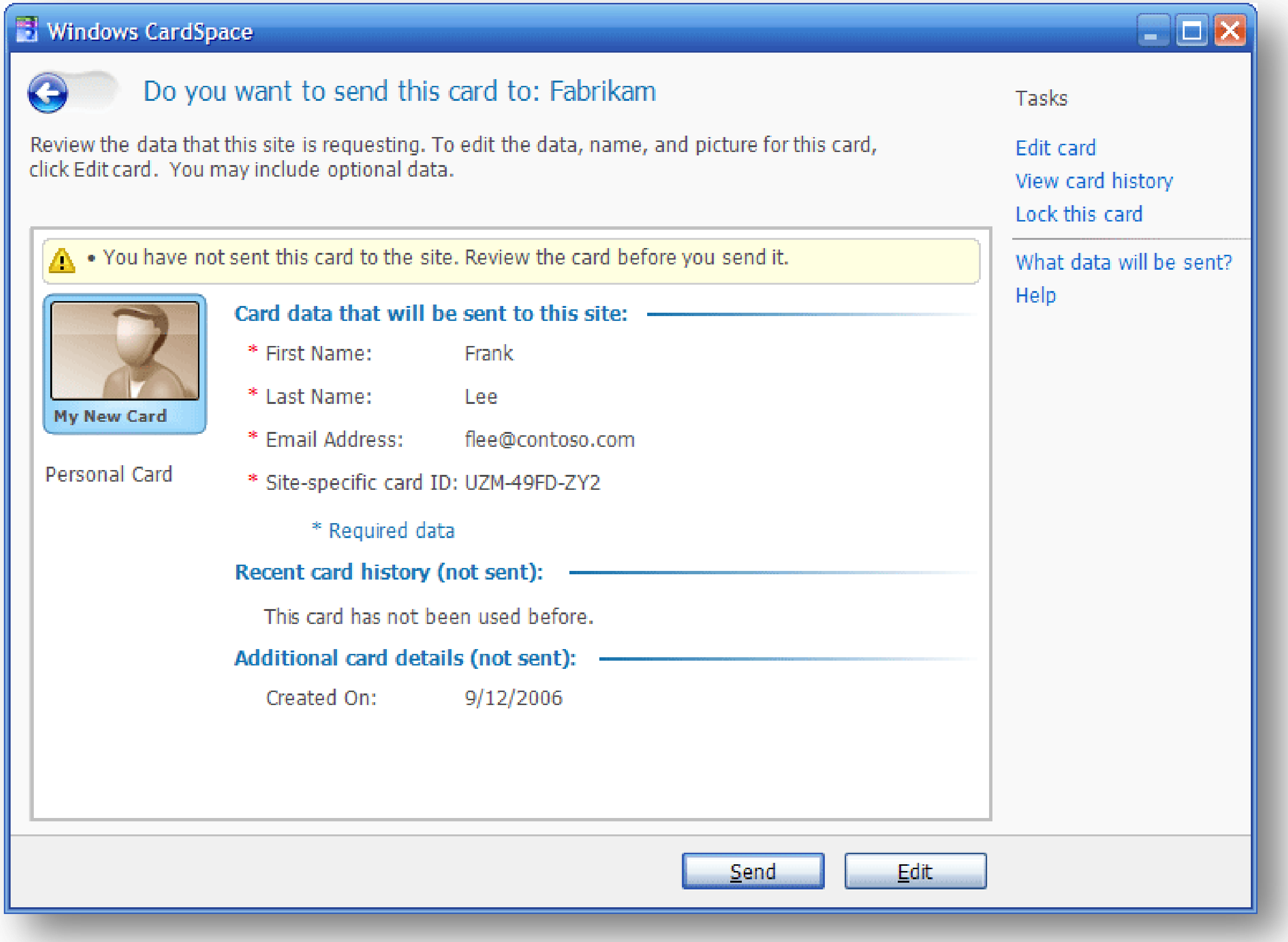
Tasks

View certificate details
View privacy statement

Disable Windows CardSpace

Why is this important?
Help

Creating a Personal Card



Do you want to send this card to: Fabrikam

Review the data that this site is requesting. To edit the data, name, and picture for this card, click Edit card. You may include optional data.

- You have not sent this card to the site. Review the card before you send it.

Personal Card

Card data that will be sent to this site:

* First Name:	Frank
* Last Name:	Lee
* Email Address:	flee@contoso.com
* Site-specific card ID:	UZM-49FD-ZY2

* Required data

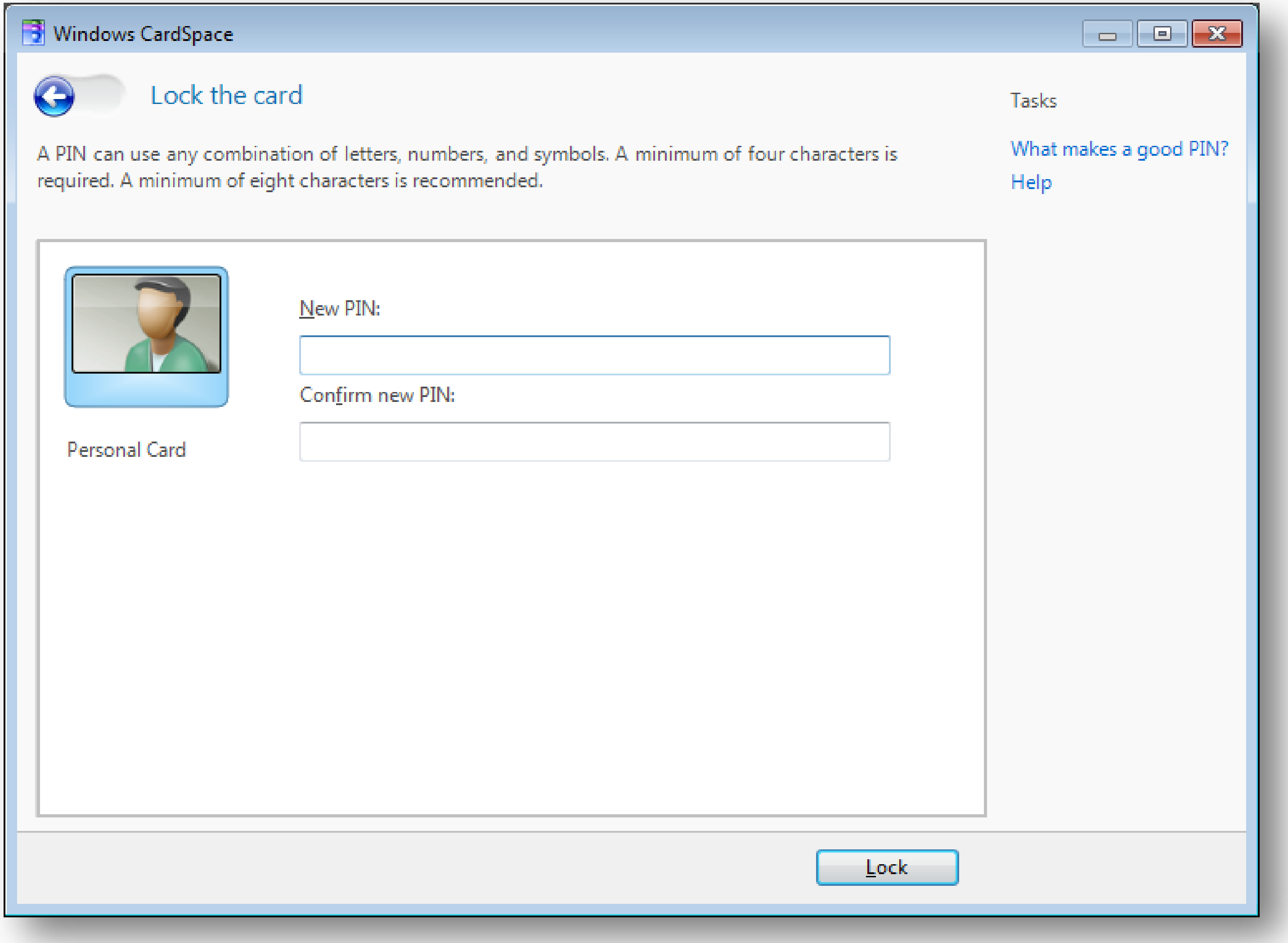
Recent card history (not sent):

This card has not been used before.

Additional card details (not sent):

Created On:	9/12/2006

Locking A Card



Windows CardSpace

Lock the card

A PIN can use any combination of letters, numbers, and symbols. A minimum of four characters is required. A minimum of eight characters is recommended.

Tasks

What makes a good PIN?

Help

Personal Card

New PIN:

Confirm new PIN:

Summary

- Brief history of user identities
- Single sign-on
- Federated identity model
- Popular identity protocols
  - SAML
  - OpenID
  - InfoCard and CardSpace